



フェデレーション認証サービス

Contents

フェデレーション認証サービス 2511	10
以前のリリース	10
参照	11
フェデレーション認証サービス 2511	12
VDAでFASアドレスリストが不要に	12
中央の常時オン追跡収集のサポート	12
修正された問題	12
既知の問題	12
サードパーティ通知	13
システム要件	14
インストールと構成	16
インストールとセットアップの順序	16
フェデレーション認証サービスをインストールする	16
FASのアップグレード	17
StoreFrontストアでFASプラグインを有効にする	18
Delivery Controller™を構成する	18
グループポリシーを構成する	18
セッション内動作	22
プロンプトの範囲	23
同意のタイムアウト	24
ロック時に切断	24
フェデレーション認証サービス管理コンソールの使用	24
証明書テンプレートを展開する	25
Active Directory 証明書サービスをセットアップする	27
フェデレーション認証サービスを承認する	28
ルールの構成	30

Citrix Cloud に接続する	35
Citrix Cloud から切断する	40
高度な構成	41
関連情報	41
FAS V2 チケットिंगとレジストリアドレスリスト	41
互換性	41
VDAが認識するFASチケットバージョン	42
StoreFrontでFAS V2チケットを構成する	43
Citrix Cloud WorkspaceでFAS V2チケットを構成する	43
その他のPowerShellの変更点	44
FASサーバーのFQDNとポートを表示する	44
コマンドレットのアドレスパラメーター	44
テナント顧客向けにフェデレーション認証サービスを有効にする	44
前提条件	44
MSP顧客の構成	45
既知の問題	47
Azure Active Directory シングルサインオン	47
ドメイン参加済み VDA	48
ハイブリッド参加済みVDA	49
認証局の構成	51
FAS で使用する複数のCAサーバーをセットアップする	51
予期される動作の変更	52
TCP アクセス用に Microsoft 証明機関を構成する	52
ユーザー証明書を事前生成する	53
Active Directoryユーザーのリストを取得する	54
FASサーバー	55
FAS承認証明書の更新	56
FAS管理コンソールの使用	56

PowerShellの使用	58
FASの認証解除とFAS証明書の削除	58
FAS管理コンソールの使用	58
PowerShellの使用	59
オフライン承認	60
関連情報	66
秘密鍵の保護	66
はじめに	66
FAS証明書とテンプレートに関する情報	67
FAS承認証明書	67
FASユーザー証明書	68
秘密鍵の保存オプション	69
キー構成PowerShellコマンド	70
構成シナリオの例	75
例1 - すべてのキーをMicrosoft Software Key Storage Providerに保存する	75
例 2 - 認証証明書キーを TPM に保存する	76
例 3 - すべてのキーを HSM に保存する	76
例 4 - 楕円曲線キーを使用する	76
秘密キー構成のテスト	77
FAS証明書の検査	78
承認証明書の検査	78
ユーザー証明書の検査	79
Citrix Virtual Apps and Desktops 2411より前のFASバージョンからのアップグレード	79
暗号化リモート処理	82
KSPリモート処理の無効化	83
メンテナンスモード	83
管理コンソールの使用	84
PowerShellの使用	84

関連情報	84
セキュリティとネットワーク構成	84
ネットワークアーキテクチャとセキュリティ	85
StoreFrontとFAS間の通信	85
VDAとFAS間の通信	86
FASとMicrosoft証明機関間の通信	86
シトリックス フェデレーテッド認証サービスとCitrix Cloud™間の接続	86
詳細情報	87
セキュリティに関する考慮事項	87
委任された登録エージェント	87
アクセス制御リストの構成	88
ファイアウォール設定	88
FAS サーバーポートの変更	88
イベントログの監視	89
ハードウェアセキュリティモジュール	89
管理者の責任	90
グループポリシー設定	90
証明書テンプレート	91
証明書テンプレートの名前を変更する	91
一般プロパティの変更	91
要求処理プロパティの変更	92
暗号化プロパティの変更	92
キー証明プロパティの変更	92
廃止されたテンプレートプロパティの変更	92
拡張プロパティの変更	92
セキュリティプロパティの変更	92
サブジェクト名のプロパティを変更する	93
サーバーのプロパティを変更する	94

発行要件のプロパティを変更する	94
互換性のプロパティを変更する	94
証明機関の管理	94
テンプレートの公開	95
ファイアウォール設定	95
登録の制限	95
ポリシーモジュールと監査	95
FAS管理	95
ACLによるStoreFront、ユーザー、およびVDAの制限	95
ルールの構成	96
証明機関とテンプレートの構成	96
セッション内証明書と認証証明書	96
秘密キーの保護とキーの長さ	97
イベントログ	97
管理アクセスと管理ツール	97
シトリックス バーチャル アプリケーションズ、シトリックス バーチャル デスクトップ、およびVDA管理者	97
一般的なWindowsサーバーのセキュリティ	97
連邦情報処理標準（FIPS）のサポート	98
関連情報	98
パフォーマンスカウンター	98
Windowsログオンの問題のトラブルシューティング	99
証明書と公開鍵インフラストラクチャ	99
UPN名と証明書のマッピング	101
Active DirectoryにおけるUPN名	101
証明書マッピングサービス	101
ログオン ドメインコントローラーの選択を制御する	101
ドメインコントローラーの選択を制御する	102

使用中のドメインコントローラーを特定する	102
アカウント監査イベントを有効にする	102
証明書検証ログ	103
証明書の有効性を確認する	103
CAPIログを有効にする	103
CAPIログ	104
エラーメッセージ	104
Kerberosログ	105
ドメインコントローラーおよびワークステーションログ	105
ドメインコントローラー CAPI2 ログ	106
ドメインコントローラー セキュリティログ	106
VDA セキュリティログ	106
VDA CAPIログ	107
VDAシステムログ	108
Windowsイベントログを使用したFASの監視	108
FASサービスは実行中ですか?	109
FASヘルスイベント	109
クラウド接続FASイベント	110
セキュリティイベント	111
FASイベントログ	112
管理イベント	112
ID アサーションの作成	115
証明書利用者として機能する	116
セッション内証明書サーバー	117
FASアサーションプラグイン	117
ワークスペース対応FAS	118
ログオン	120
セッション内証明書	120

証明書要求とキーペアの生成	121
エンドユーザーのエラーメッセージ	122
FAS 常時トレース	122
常時トレースの収集	123
常時トレースの無効化	123
常時トレースを中央ログサーバーに送信する	123
関連情報	123
PowerShell コマンドレット	123
FASインストーラーオプション	124
FASをインストールするためのコマンドラインオプション	124
Windows Server CoreへのFASのインストール	125
Windows Server CoreでのFAS管理	126
展開アーキテクチャ	127
はじめに	127
アーキテクチャの概要	127
内部展開	128
Citrix Gateway の展開	131
ADFS SAML展開	134
B2Bアカウントマッピング	135
Windows 10 Azure AD への参加	136
ADFS展開	138
はじめに	138
SAMLの概要	140
リダイレクトURL	140
識別子	140
戻りアドレス	140
署名証明書	140
シングルサインアウトURL	141

構成	141
SAMLポリシーを記入する	141
関連情報	142

フェデレーション認証サービス 2511

フェデレーション認証サービス (FAS) は、Active Directory証明書サービスと統合するように設計された特権コンポーネントです。ユーザーに証明書を動的に発行し、スマートカードを持っているかのようにActive Directory環境にログオンできるようにします。これにより、StoreFront™は、SAML (Security Assertion Markup Language) アサーションなど、より広範な認証オプションを使用できます。SAMLは、インターネット上で従来のWindowsユーザーアカウントの代替として一般的に使用されます。

フェデレーション認証サービス 2511 は、FASの最新のCurrent Releaseバージョンです。この記事では、この最新リリースにおける機能と構成について説明します。

以前のリリース

以前のFASリリースのドキュメントについては、以下を参照してください。

- [フェデレーション認証サービス 2507 LTSR](#)
- [フェデレーション認証サービス 2503](#)
- [フェデレーション認証サービス 2411](#)
- [フェデレーション認証サービス 2407](#)
- [フェデレーション認証サービス 2402 LTSR](#)
- [フェデレーション認証サービス 2311](#)
- [フェデレーション認証サービス 2308](#)
- [フェデレーション認証サービス 2305](#)
- [フェデレーション認証サービス 2303](#)
- [フェデレーション認証サービス 2212](#)
- 「フェデレーション認証サービス 2209」 ([/ja-jp/federated-authentication-service/2209.html](#))
- 「フェデレーション認証サービス 2206」 ([/ja-jp/federated-authentication-service/2206.html](#))
- 「フェデレーション認証サービス 2203 LTSR」 ([/ja-jp/federated-authentication-service/2203-ltsr.html](#))
- 「フェデレーション認証サービス 2112」 ([/ja-jp/federated-authentication-service/2112.html](#))

- 「フェデレーション認証サービス 2109」 (</ja-jp/federated-authentication-service/2109.html>)
- 「フェデレーション認証サービス 2106」 (</ja-jp/federated-authentication-service/2106.html>)
- 「フェデレーション認証サービス 2103」 (</ja-jp/federated-authentication-service/2103.html>)
- 「フェデレーション認証サービス 1912 LTSR」 (</ja-jp/federated-authentication-service/1912-ltsr.html>)
- [XenAppおよびXenDesktop 7.15 長期サービスリリース](#)

Current Releases (CR)およびLong Term Service Releases (LTSR)の製品ライフサイクル戦略については、[ライフサイクルマイルストーン](#)で説明されています。

参照

- [Active Directory 証明書サービス概要](#)
- [証明書ログオン用にWindowsを構成する](#)

フェデレーション認証サービス 2511

このフェデレーション認証サービス (FAS) のリリースには、以下の新機能が含まれています。バグ修正については、[修正された問題](#)を参照してください。

VDAでFASアドレスリストが不要に

Citrix Virtual Apps and Desktops 2511リリースでは、**FAS V2チケットティング**として知られる新しいFASチケット形式をサポートしています。

展開環境のFASサーバーとVDAがCitrix Virtual Apps and Desktops 2511以降を実行している場合、VDAのレジストリにFASアドレスリストは不要になります。

詳細については、[FAS V2チケットティングとレジストリアドレスリスト](#)を参照してください。

中央の常時オン追跡収集のサポート

常時オン追跡により、FASはそのアクティビティをファイルシステムにログ記録します。この機能はトラブルシューティングに役立ち、発生したインシデントを再現する必要性を排除できる可能性があります。

このリリースでは、展開環境の中央サーバーに常時オン追跡を自動的に送信できます。

詳細については、[FAS常時オン追跡](#)を参照してください。

修正された問題

- FASのロック時に切断が有効になっているCitrix Virtual Apps and Desktopsのセッションローミングが確実に機能するようになりました。この修正はFAS VDAプラグインに含まれています。

既知の問題

以下の操作を行うと、VDA上のレジストリベースのFASグループポリシーが削除され、シングルサインオンの失敗が発生します。

- VDAをCitrix Virtual Apps and Desktops 2411から将来のバージョンにアップグレードする

- VDAをCitrix Virtual Apps and Desktops 2503から将来のバージョンにアップグレードする
- VDAからCitrix Virtual Apps and Desktops 2411をアンインストールする
- VDAからCitrix Virtual Apps and Desktops 2503をアンインストールする

FASグループポリシーを復元するには、VDAで以下のコマンドを実行します。

```
gpupdate /force
```

サードパーティ通知

このFederated Authentication Serviceリリースには、以下のドキュメントに定義されている条件に基づいてライセンス供与されたサードパーティ製ソフトウェアが含まれる場合があります。

- [Citrix Virtual Apps and Desktops サードパーティ通知 \(PDFダウンロード\)](#)
- [FlexNet Publisher 2017 \(11.15.0.0\) の非商用ソフトウェア開示 \(PDFダウンロード\)](#)
- [FlexNet Publisher 11.15.0 で使用されている FlexNet Publisher ドキュメント補足 サードパーティおよびオープンソースソフトウェア \(PDFダウンロード\)](#)

システム要件

- Federated Authentication Service (FAS) は、以下の Windows Server バージョンでサポートされています。
 - Windows Server 2025、スタンダード、およびデータセンターエディション
 - Windows Server 2022、スタンダード、およびデータセンターエディション
 - Windows Server 2019、Standard および Datacenter Edition、および Server Core オプション
- Citrix は、他の Citrix コンポーネントがインストールされていないサーバーに FAS をインストールすることを推奨します。
- Windows Server は、登録機関証明書と秘密キーにアクセスできるため、セキュリティで保護されている必要があります。証明書と秘密キーにより、サーバーはドメインユーザーの証明書を発行できます。サーバーは、発行されたドメインユーザー証明書と秘密キーにもアクセスできます。
- FAS の [PowerShell コマンドレット](#) には、FAS サーバーに Windows PowerShell 64 ビットがインストールされている必要があります。
- ユーザー証明書を発行するには、Microsoft Enterprise Certificate Authority またはその他の検証済み Certificate Authority (CA) が必要です。以下の非 Microsoft PKI プロバイダーは、FAS で使用するためのソリューションを検証済みです。これらの検証に関するサポートについては、ベンダーにお問い合わせください。
 - キーファクター コマンド
 - セクティゴ サーティフィケート マネージャー
 - ベナフィ ゼロタッチ PKI
 - HDI PKIaaS (ベナフィ)
 - エントラスト WNES
 - AppViewX
 - エバートラスト ホライズン CLM
 - オープントラスト PKI
 - IDノミック PKI-3

- デジサート 自動登録サーバー
- Microsoft以外のCAでFASを使用するためのサポートとガイダンスについては、関連するPKIプロバイダーにお問い合わせください。
- Microsoft以外の証明機関については、以下を確認してください。
 - 証明機関 (CA) が登録サービスとしてActive Directoryに登録されていること。
 - CA証明書がドメインコントローラーのNTAuthストアにあること。詳細については、[「サードパーティの証明機関 \(CA\) 証明書をEnterprise NTAuthストアにインポートする方法」](#)を参照してください。
- 詳細については、「[展開ガイド：Citrix Federated Authentication ServiceおよびSectigo MS Agent](#)」を参照してください。

Citrix Virtual AppsまたはCitrix Virtual Desktops™サイトの場合：

- Delivery Controller、Virtual Delivery Agent (VDA)、およびStoreFront™サーバーはすべて、サポートされているバージョンである必要があります。

このサービスの展開を計画する際は、「[セキュリティに関する考慮事項](#)」セクションを確認してください。

インストールと構成

インストールとセットアップの順序

1. フェデレーション認証サービス (FAS) をインストールする(/ja-jp/federated-authentication-service/2511/install-configure.html#install-the-federated-authentication-service)
2. StoreFrontストアでFASプラグインを有効にする(/ja-jp/federated-authentication-service/2511/install-configure.html#enable-the-fas-plugin-on-storefront-stores)
3. Delivery Controllerを構成する(/ja-jp/federated-authentication-service/2511/install-configure.html#configure-the-delivery-controller)
4. グループポリシーを構成する(/ja-jp/federated-authentication-service/2511/install-configure.html#configure-group-policy)
5. FAS管理コンソールを使用して、次の操作を行います。
 - a. 証明書テンプレートを展開する(/ja-jp/federated-authentication-service/2511/install-configure.html#deploy-certificate-templates)
 - b. 証明機関をセットアップする(/ja-jp/federated-authentication-service/2511/install-configure.html#set-up-active-directory-certificate-services)
 - c. FASが証明機関を使用することを承認する(/ja-jp/federated-authentication-service/2511/install-configure.html#authorize-federated-authentication-service)
 - d. ルールを構成する(/ja-jp/federated-authentication-service/2511/install-configure.html#configure-rules)
 - e. FASをCitrix Cloudに接続する(/ja-jp/federated-authentication-service/2511/install-configure.html#connect-to-citrix-cloud) (オプション)

フェデレーション認証サービスをインストールする

セキュリティのため、Citrixではフェデレーション認証サービス (FAS) を専用サーバーにインストールすることをお勧めします。このサーバーは、ドメインコントローラーまたは証明機関と同様の方法で保護する必要があります。FASは、次のいずれかからインストールできます。

- ISOが挿入されたときに自動実行スプラッシュ画面の**Federated Authentication Service**ボタンから、Citrix Virtual Apps and Desktops™インストーラー

- `XenDesktopFasSetup.exe` は、Citrix Virtual Apps and Desktops ISO の `x64\XenDesktopSetup\XenDesktopFasSetup.exe` に格納されています。
- スタンドアロンFASインストーラーファイルである `FasSetup_xxxx.exe` は、[Citrix Downloads](#) で入手できます。

これらのいずれかをインストールすると、以下のコンポーネントがインストールされます。

- フェデレーション認証サービス
- 高度なFAS構成のための [PowerShell snap-in cmdlets](#)
- [FAS管理コンソール](#)
- FASグループポリシーテンプレート (CitrixFederatedAuthenticationService.admx または CitrixFederatedAuthenticationService.adml)
- 証明書テンプレートファイル
- [パフォーマンスカウンター](#) と [イベントログ](#)
- FASの常時トレースをサポートするCitrix Telemetry Service
- 常時トレースなどの診断情報を収集するために使用できるアプリケーションである [Citrix Scout](#)

インストーラーの詳細については、[FASのインストール用コマンドラインオプション](#) を参照してください。

FASのアップグレード

インプレースアップグレードを使用して、FASを新しいバージョンにアップグレードできます。アップグレードする前に、次の点を考慮してください。

- インプレースアップグレードを実行すると、すべてのFASサーバー設定が保持されます。
- FASをアップグレードする前に、FAS管理コンソールを閉じてください。
- 常に少なくとも1つのFASサーバーが利用可能であることを確認してください。Federation Authentication Serviceが有効なStoreFront™サーバーからどのサーバーにも到達できない場合、ユーザーはログオンしたりアプリケーションを起動したりできません。

アップグレードを開始するには、Citrix Virtual Apps and DesktopsインストーラーまたはスタンドアロンのFASインストーラーファイルからFASをインストールします。

StoreFrontストアでFASプラグインを有効にする

注：

Citrix CloudでのみFASを使用している場合、この手順は不要です。

StoreFrontストアでFASプラグインを有効にする方法の詳細については、<https://docs.citrix.com/ja-jp/storefront/current-release/configure-authentication-and-delegation/fas>を参照してください。

Delivery Controller™を構成する

注：

Citrix CloudでのみFASを使用している場合、この手順は不要です。

FASを使用するには、Citrix Virtual AppsまたはCitrix Virtual Desktops™ Delivery Controllerが接続先のStoreFrontサーバーを信頼するように構成します。これには、**Set-BrokerSite -TrustRequestsSentToTheXmlServicePort \$true** PowerShellコマンドレットを実行します。このコマンドは、サイト内のDelivery Controllerの数に関係なく、サイトごとに1回実行します。

グループポリシーを構成する

注：

すべてのFASサーバーとVDAがバージョン2511以降の場合、VDA上のグループポリシーFQDNリストは不要になります。[FAS V2チケットティングとレジストリアドレスリスト](#)を参照してください。

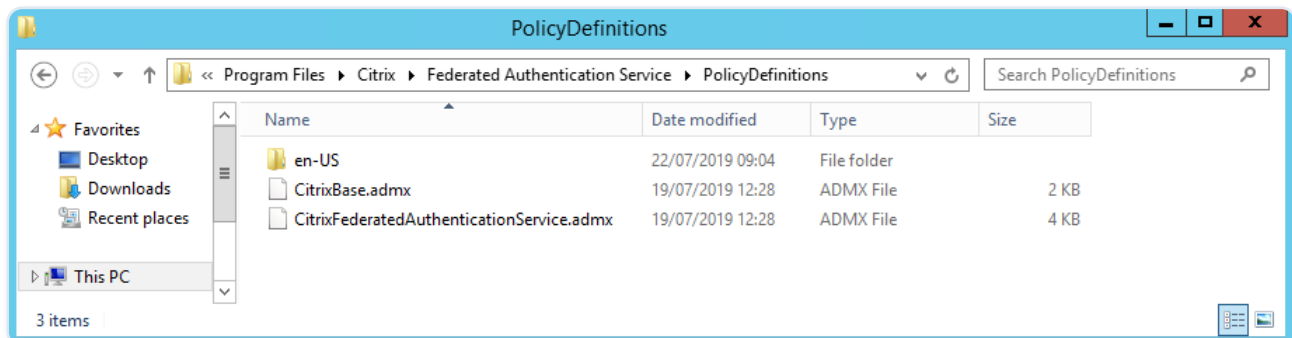
FASをインストールした後、インストールで提供されるグループポリシーテンプレートを使用して、グループポリシー内のサーバーの完全修飾ドメイン名（FQDN）を指定します。

重要:

チケットを要求するStoreFrontサーバーと、チケットを引き換えるVirtual Delivery Agent（VDA）が、Group Policy objectによって適用される自動サーバー番号付けを含め、FQDNの同一の構成を持つことを確認してください。

簡素化のため、以下の例では、すべてのマシンに適用される単一のポリシーをドメインレベルで構成しています。ただし、これは必須ではありません。FASは、StoreFrontサーバー、VDA、およびFAS管理コンソールを実行しているマシンが同じFQDNのリストを参照できる限り機能します。手順6を参照してください。

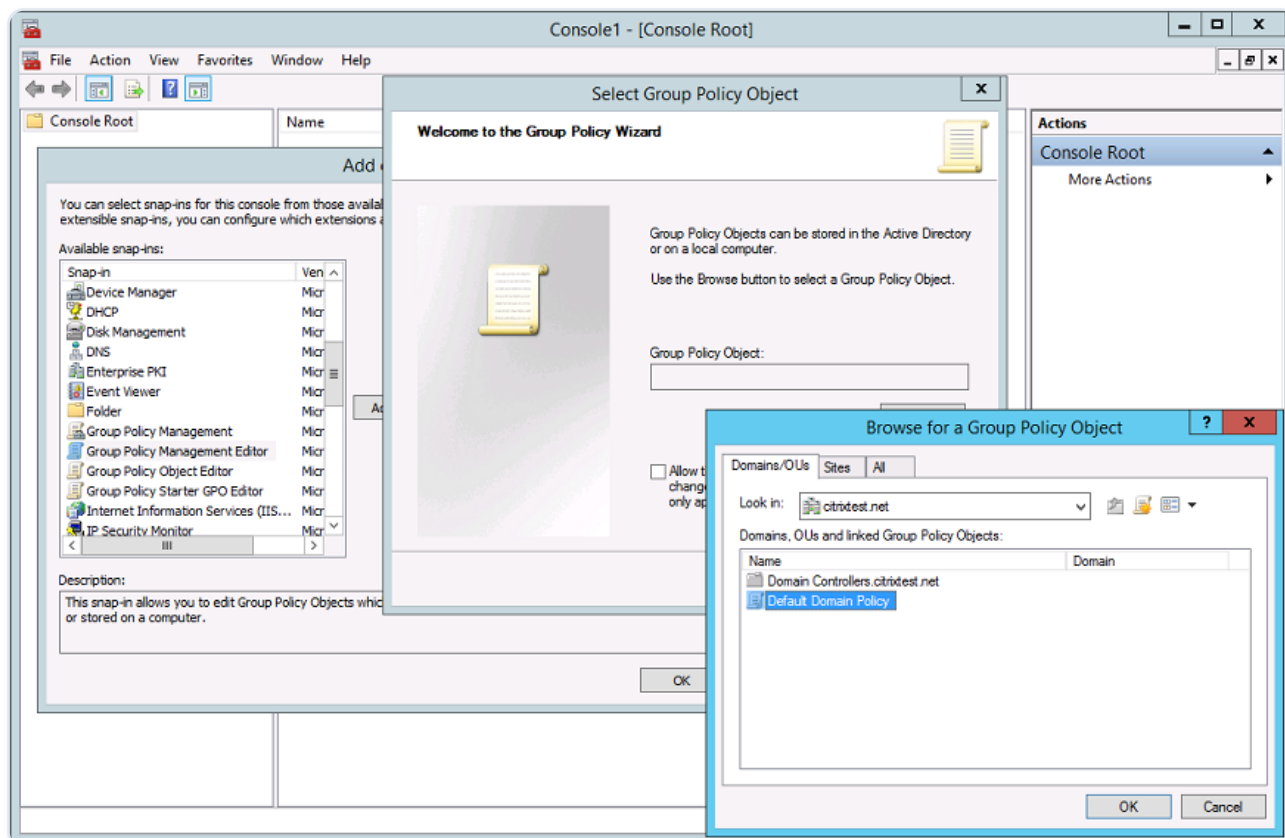
手順1. FASをインストールしたサーバーで、C:\Program Files\Citrix\Federated Authentication Service\PolicyDefinitions\CitrixFederatedAuthenticationService.admx ファイルと CitrixBase.admx ファイル、および en-US フォルダーを探します。



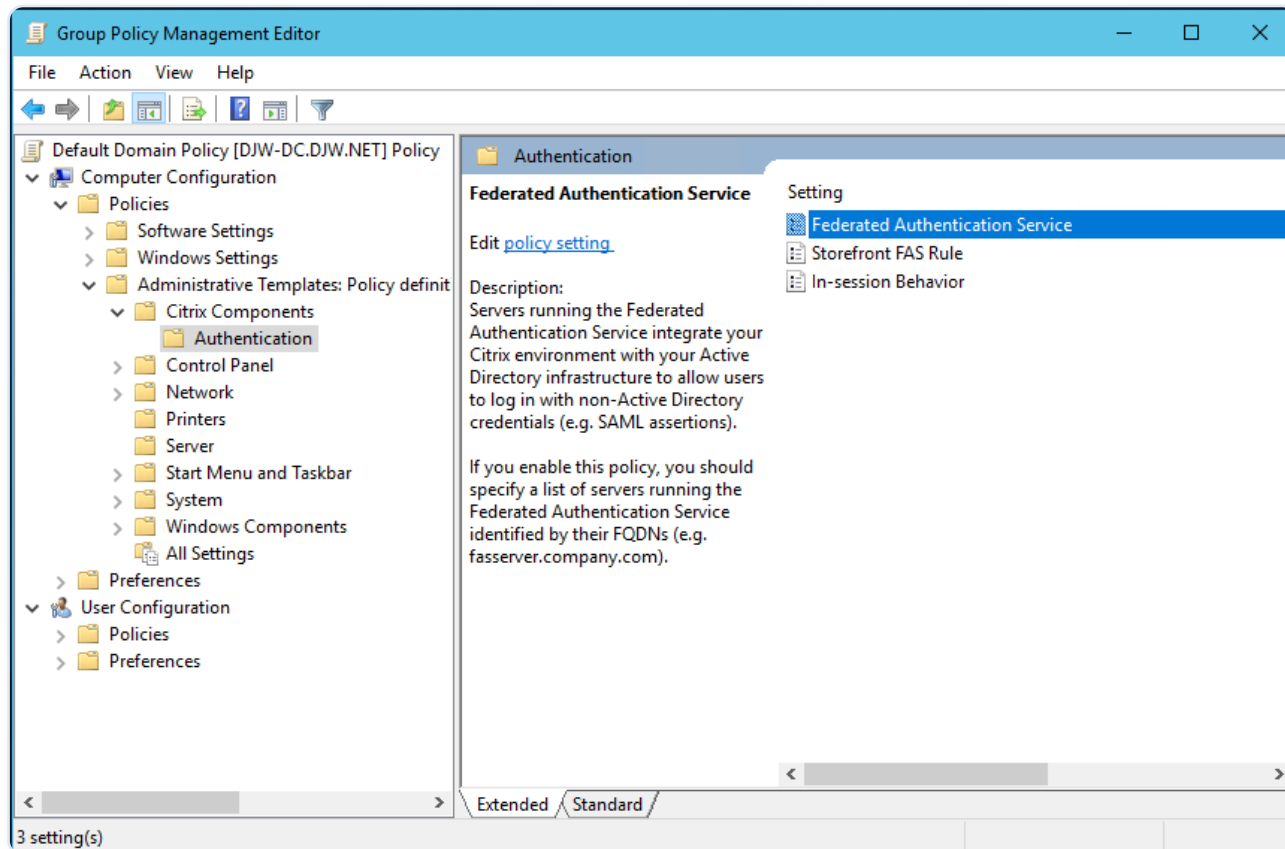
手順2. これらのファイルをドメインコントローラーにコピーし、C:\Windows\PolicyDefinitionsおよびen-USサブフォルダーに配置します。

手順3. Microsoft Management Console（コマンドラインからmmc.exe）を実行します。メニューバーから、**ファイル > スナップインの追加と削除**を選択します。**グループポリシー管理エディター**を追加します。

グループポリシーオブジェクトを求められたら、**参照**を選択し、**Default Domain Policy**を選択します。または、ご使用の環境に適したポリシーオブジェクトを、お好みのツールを使用して作成および選択することもできます。このポリシーは、影響を受けるCitrixソフトウェア（VDA、StoreFrontサーバー、管理ツール）を実行しているすべてのマシンに適用する必要があります。



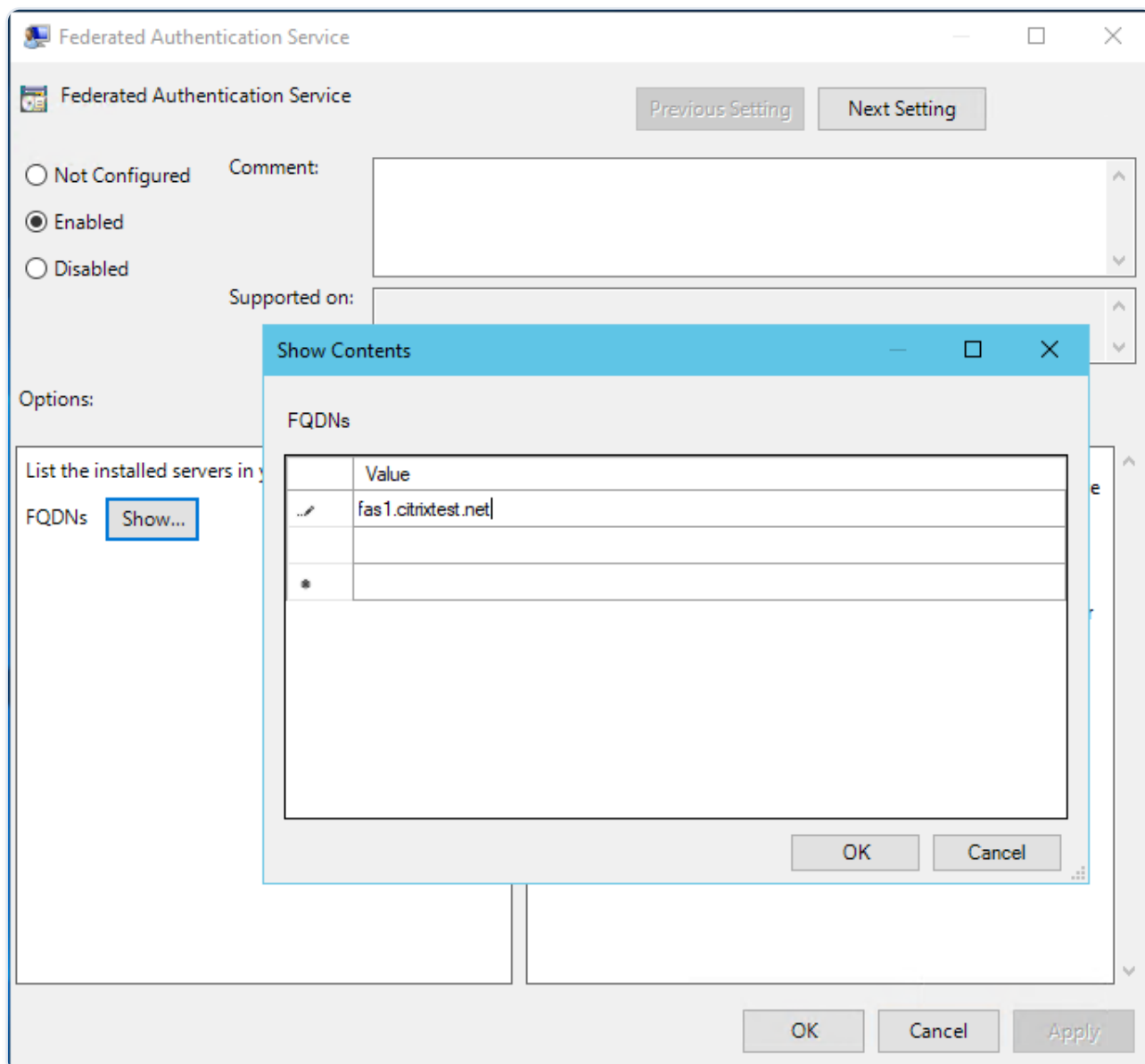
手順4. Computer Configuration/Policies/Administrative Templates/Citrix Components/Authenticationにある*Federated Authentication Service*ポリシーに移動します。



注：

Federated Authentication Serviceポリシー設定は、CitrixBase.admx/CitrixBase.admlテンプレートファイルをPolicyDefinitionsフォルダーに追加した場合にのみ、ドメインGPOで利用可能です。手順3の後、Federated Authentication Serviceポリシー設定は、**管理用テンプレート > Citrixコンポーネント > 認証フォルダー**に表示されます。

手順5. Federated Authentication Serviceポリシーを開き、**有効**を選択します。これにより、**表示**ボタンを選択できるようになり、FASサーバーのFQDNを構成できます。



ステップ 6. FASサーバーのFQDNを入力します。

重要:

複数のFQDNを入力する場合、VDA、StoreFrontサーバー（存在する場合）、およびFASサーバーから見て、リストの順序は一貫している必要があります。[グループポリシー設定](#)を参照してください。

ステップ 7. グループポリシーウィザードを終了してグループポリシーの変更を適用するには、**OK**をクリックします。変更を有効にするには、マシンを再起動するか（またはコマンドラインから **gpupdate /force**を実行する）必要がある場合があります。

セッション内動作

このポリシーは、ユーザーのVDAセッションでエージェントプロセスをアクティブ化し、セッション内証明書、同意、およびロック時の切断をサポートします。セッション内証明書は、このポリシーが有効になっており、かつ証明書の作成に使用されたFASルールでセッション内使用が許可されている場合にのみ利用可能です。[ルールの構成](#)を参照してください。

有効にすると、このポリシーが有効になり、FASエージェントプロセスがユーザーのVDAセッションで実行されることが許可されます。

無効にすると、このポリシーが無効になり、FASエージェントプロセスが実行されないようにします。

プロンプトの範囲

このポリシーが有効になっている場合、**プロンプトの範囲**は、アプリケーションがセッション内証明書を使用することを許可するための同意をユーザーに求める方法を制御します。次の3つのオプションがあります。

- **同意不要**—このオプションはセキュリティプロンプトを無効にし、秘密鍵はサイレントに使用されます。
- **プロセスごとの同意**—実行中の各プログラムが個別に同意を求めます。

- **セッションごとの同意**—ユーザーが**OK**をクリックすると、このオプションはセッション内のすべてのプログラムに適用されます。

同意のタイムアウト

このポリシーが有効な場合、**同意タイムアウト**は、同意が持続する期間（秒単位）を制御します。たとえば、300秒に設定すると、ユーザーは5分ごとにプロンプトを表示されます。値がゼロの場合、プライベートキー操作ごとにユーザーにプロンプトが表示されます。

ロック時に切断

このポリシーが有効な場合、ユーザーが画面をロックすると、ユーザーセッションは自動的に切断されます。この動作は、「スマートカード取り外し時に切断」ポリシーに似ています。ユーザーがActive Directoryログオン資格情報を持っていない場合に、この機能を使用します。

注：

ロック時に切断するポリシーは、VDA上のすべてのセッションに適用されます。

フェデレーション認証サービス管理コンソールの使用

注：

FAS管理コンソールはほとんどの展開に適していますが、PowerShellインターフェイスはより高度なオプションを提供します。FAS PowerShellコマンドレットの詳細については、「[PowerShellコマンドレット](#)」を参照してください。

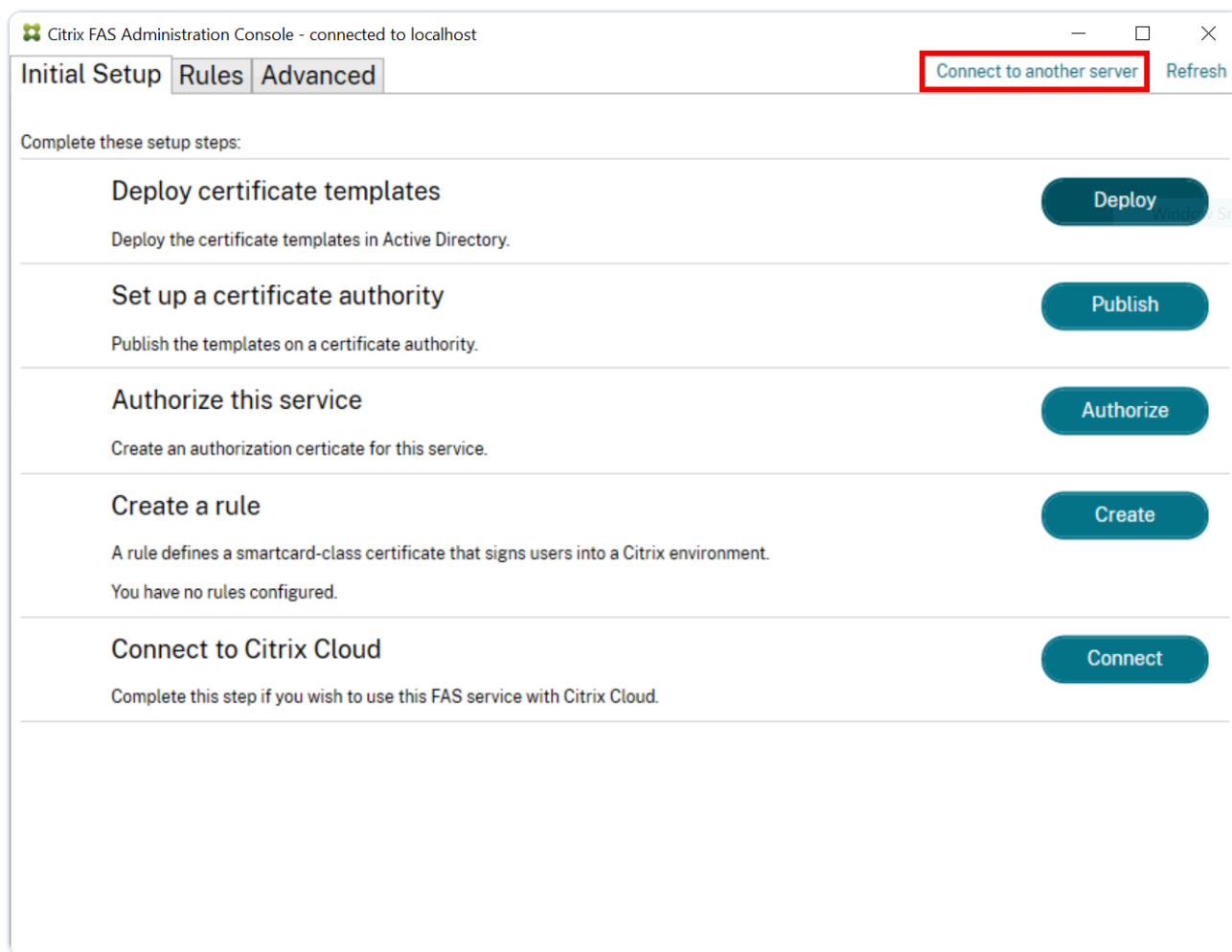
FAS管理コンソールは、FASの一部としてインストールされます。アイコン（Citrix Federated Authentication Service）がスタートメニューに配置されます。

管理コンソールを初めて使用する際には、次のプロセスがガイドされます。

- 証明書テンプレートを展開します。
- 証明機関をセットアップします。
- FASが証明機関を使用することを承認します。

OS構成ツールを使用して、一部の手順を手動で完了することもできます。

FAS管理コンソールは、デフォルトでローカルFASサービスに接続します。必要に応じて、コンソールの右上にある**別のサーバーに接続**を使用して、リモートサービスに接続できます。

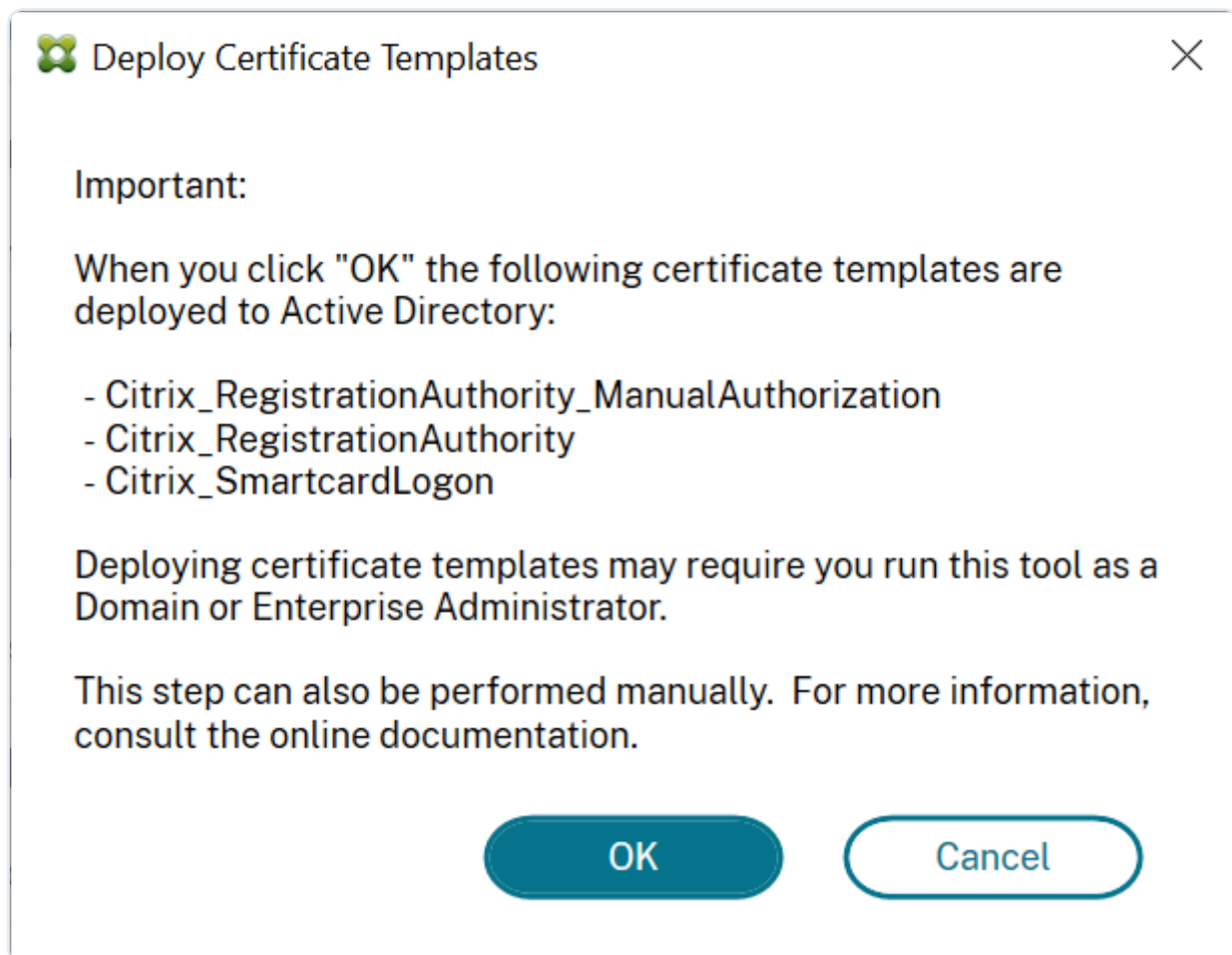


証明書テンプレートを展開する

他のソフトウェアとの相互運用性の問題を避けるため、FAS は独自の用途のために 3 つの Citrix 証明書テンプレートを提供します。

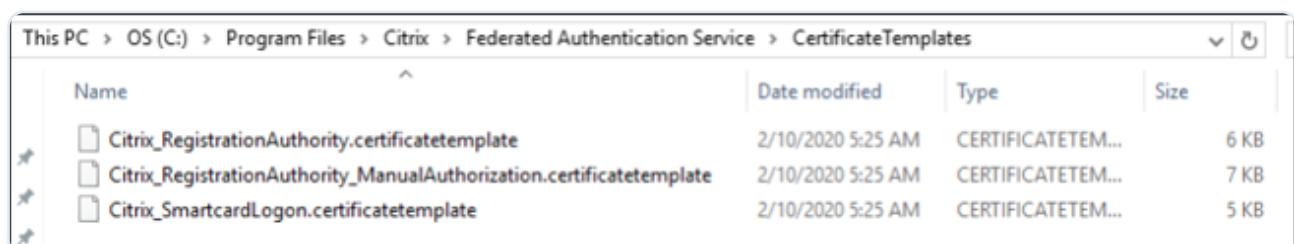
- Citrix_RegistrationAuthority_ManualAuthorization
- Citrix_RegistrationAuthority
- Citrix_SmartcardLogon

これらのテンプレートは Active Directory に登録する必要があります。展開ボタンをクリックし、OKをクリックします。



テンプレートの構成は、FAS とともにインストールされる拡張子 .certificatetemplate の XML ファイルにあります。

C:\プログラムファイル\シトリックス\フェデレーション認証サービス\証明書テンプレート



これらのテンプレートファイルをインストールする権限がない場合は、Active Directory 管理者に渡してください。

テンプレートを手動でインストールするには、テンプレートが含まれるフォルダーから次の PowerShell コマンドを実行します。

```
$template =
[System.IO.File]::ReadAllBytes("$Pwd\Citrix_SmartcardLogon.certificatetemp
late")

$CertEnrol = New-Object -ComObject
```

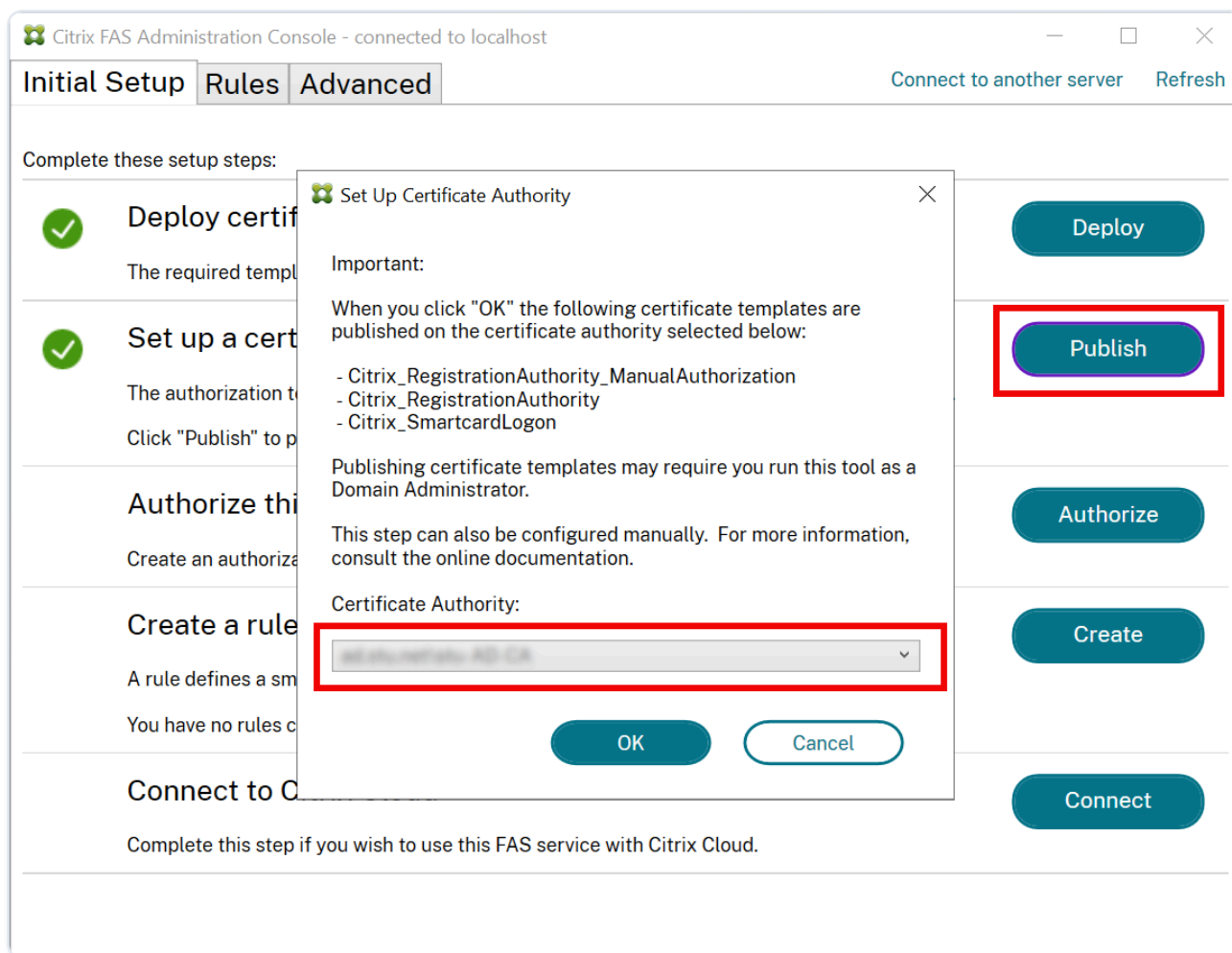
```
X509Enrollment.CX509EnrollmentPolicyWebService  
  
$CertEnrol.InitializeImport($template)  
  
$comtemplate = $CertEnrol.GetTemplates().ItemByIndex(0)  
  
$writabletemplate = New-Object -ComObject  
X509Enrollment.CX509CertificateTemplateADWritable  
  
$writabletemplate.Initialize($comtemplate)  
  
$writabletemplate.Commit(1, $NULL)
```

Active Directory 証明書サービスをセットアップする

Citrix 証明書テンプレートをインストールした後、それらを 1 つ以上の Microsoft Enterprise 証明機関サーバーに公開する必要があります。Active Directory 証明書サービスを展開する方法については、Microsoft のドキュメントを参照してください。

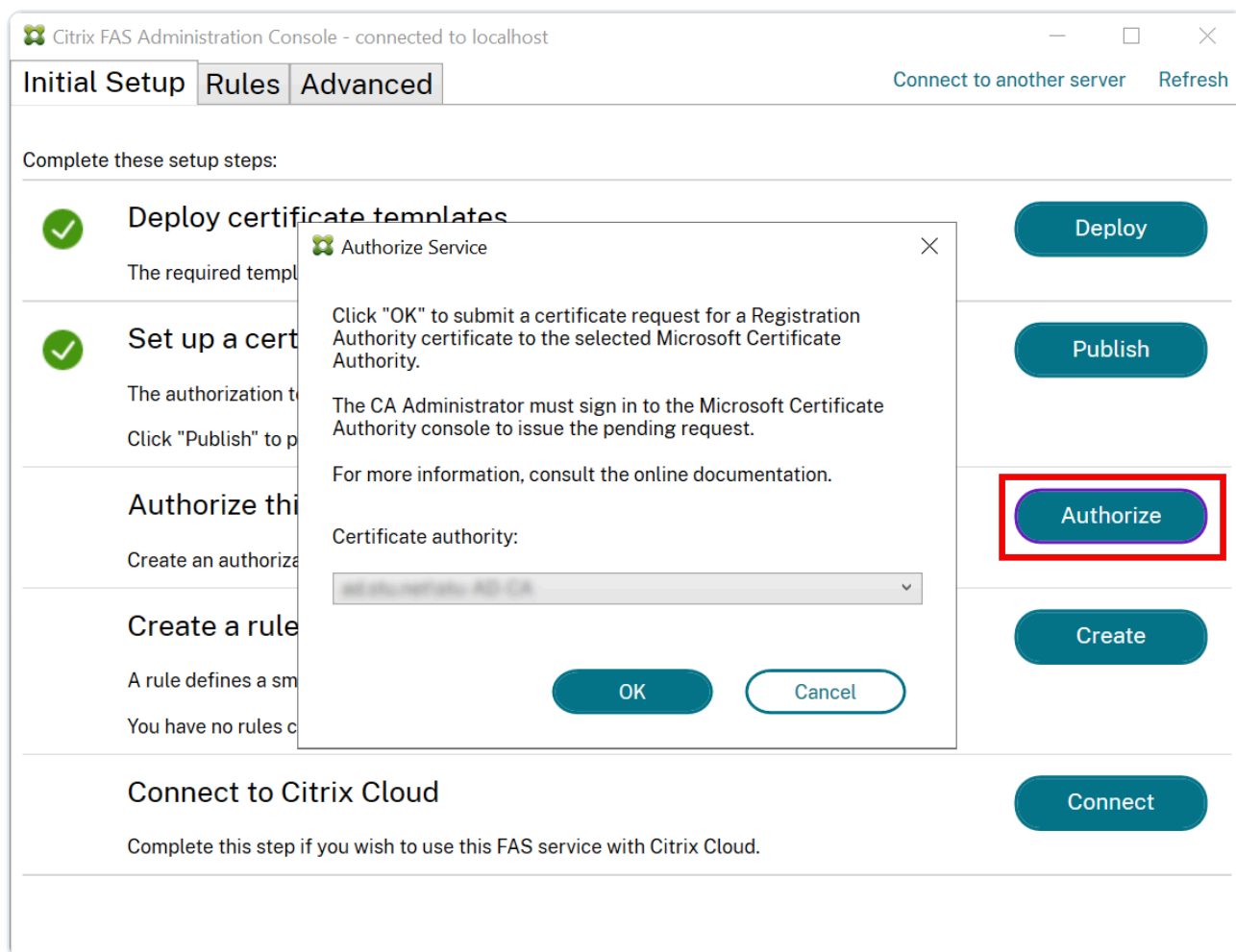
認証局を管理する権限を持つユーザーは、少なくとも1つのサーバーにテンプレートを公開する必要があります。それらを公開するには、**Set Up Certificate Authority** を使用します。

(証明書テンプレートは、Microsoft Certification Authority コンソールを使用して公開することもできます。)



フェデレーション認証サービスを承認する

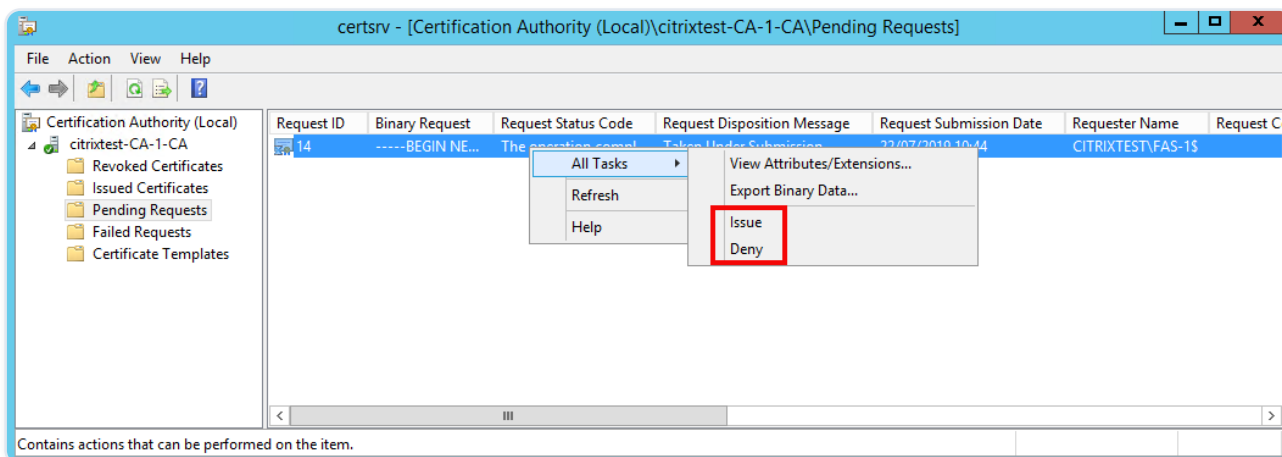
この手順により、FAS の承認が開始されます。管理コンソールは、Citrix_RegistrationAuthority_ManualAuthorization テンプレートを使用して証明書要求を生成し、そのテンプレートを公開している認証局のいずれかに送信します。



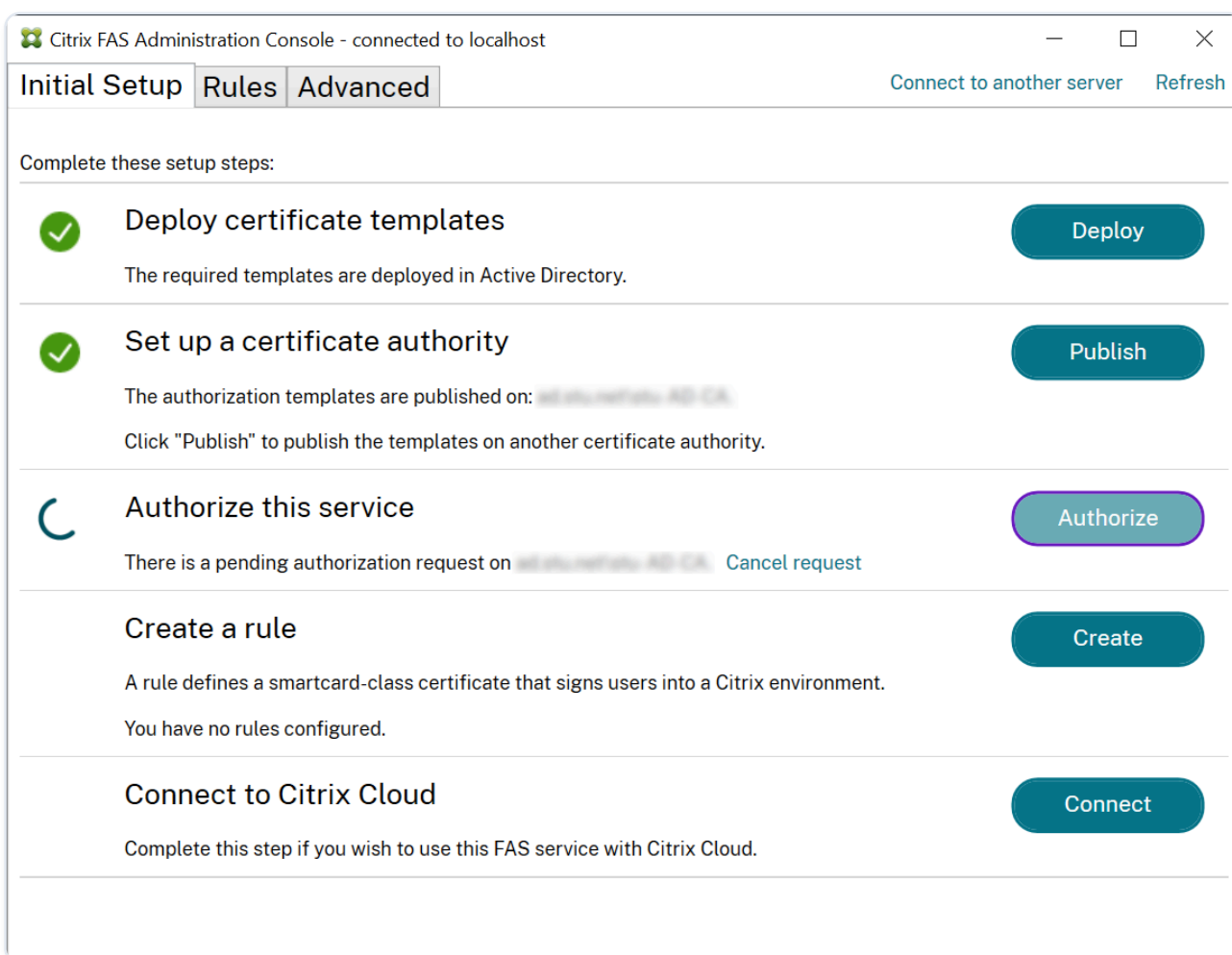
要求が送信されると、Microsoft Certification Authority コンソールの **Pending Requests** リストに、FAS マシンアカウントからの保留中の要求として表示されます。FAS の構成を続行する前に、認証局管理者はその要求を発行または拒否する必要があります。

管理者が **Issue** または **Deny** を選択するまで、FAS 管理コンソールはビジー状態の「スピナー」を表示します。

Microsoft Certification Authority コンソールで、**All Tasks** を右クリックし、証明書要求に対して **Issue** または **Deny** を選択します。**Issue** を選択すると、FAS 管理コンソールに承認証明書が表示されます。**Deny** を選択すると、コンソールにエラーメッセージが表示されます。



FAS 管理コンソールは、このプロセスが完了したことを自動的に検出します。これには数分かかる場合があります。



ルールの構成

FAS は、StoreFront の指示に従って、VDA ログオンおよびセッション内使用の証明書の発行を承認するためにルールを使用します。

各ルールは以下を指定します。

- 証明書を要求することを信頼されているStoreFrontサーバー。
- 証明書が要求されるユーザーのセット。
- 証明書の使用が許可されているVDAマシンのセット。

Citrixでは、「default」という名前のルールを作成することをお勧めします。これは、StoreFrontがFASに接続する際に、同じ名前のルールを要求するためです。

異なる証明書テンプレートや証明機関を参照するカスタムルールをさらに作成し、異なるプロパティと権限を持つように構成できます。これらのルールは、異なるStoreFrontサーバーまたはWorkspaceで使用するように構成できます。グループポリシー構成オプションを使用して、StoreFrontサーバーがカスタムルールを名前で要求するように構成します。

作成（または「ルール」タブの**ルールの作成**）をクリックして、ルールを作成するための情報を収集するルール作成ウィザードを開始します。「ルール」タブには、各ルールの概要が表示されます。

Citrix FAS Administration Console - connected to localhost

Initial Setup Rules Advanced [Connect to another server](#) [Refresh](#)

A rule defines a smartcard-class certificate that signs users into a Citrix environment.

[+ Create rule](#)

Default	Summary
	Rule name: Default
	Status: OK
	Template: Citrix_SmartcardLogon
	Certificate authorities: add this certificate AD-CA
	Certificate available in-session: No
	Access control: Configured
	Restrictions: Not configured
	Cloud rule: No

ウィザードは次の情報を収集します。

テンプレート: ユーザー証明書の発行に使用される証明書テンプレート。これは Citrix_SmartcardLogonテンプレート、またはその変更されたコピーである必要があります（[証明書テンプレート](#)を参照）。

証明機関: ユーザー証明書を発行し、テンプレートを公開する証明機関。FASは、フェールオーバーと負荷分散のために複数の証明機関の追加をサポートしています。選択した証明機関のステータスが「テンプレート利用可能」と表示されていることを確認してください。[証明機関の管理](#)を参照してください。

セッション内使用: セッション内使用を許可オプションは、VDAへのログオン後に証明書を使用できるかどうかを制御します。

- **セッション内使用を許可**が選択されていない場合（デフォルト、*推奨*）—証明書はログオンまたは再接続にのみ使用され、ユーザーは認証後に証明書にアクセスできません。
- **セッション内使用を許可**が選択されている場合—ユーザーは認証後に証明書にアクセスできます。ほとんどのお客様はこのオプションを選択すべきではありません。イントラネットWebサイトやファイル共有など、VDAセッション内からアクセスされるリソースは、Kerberosシングルサインオンを使用してアクセスできるため、セッション内証明書は必要ありません。

セッション内使用を許可を選択した場合、[セッション内動作グループポリシー](#)も有効にしてVDAに適用する必要があります。証明書は、ログオン後にアプリケーションで使用するためにユーザーの個人証明書ストアに配置されます。たとえば、VDAセッション内のWebサーバーへのTLS認証が必要な場合、Internet Explorerはその証明書を使用します。

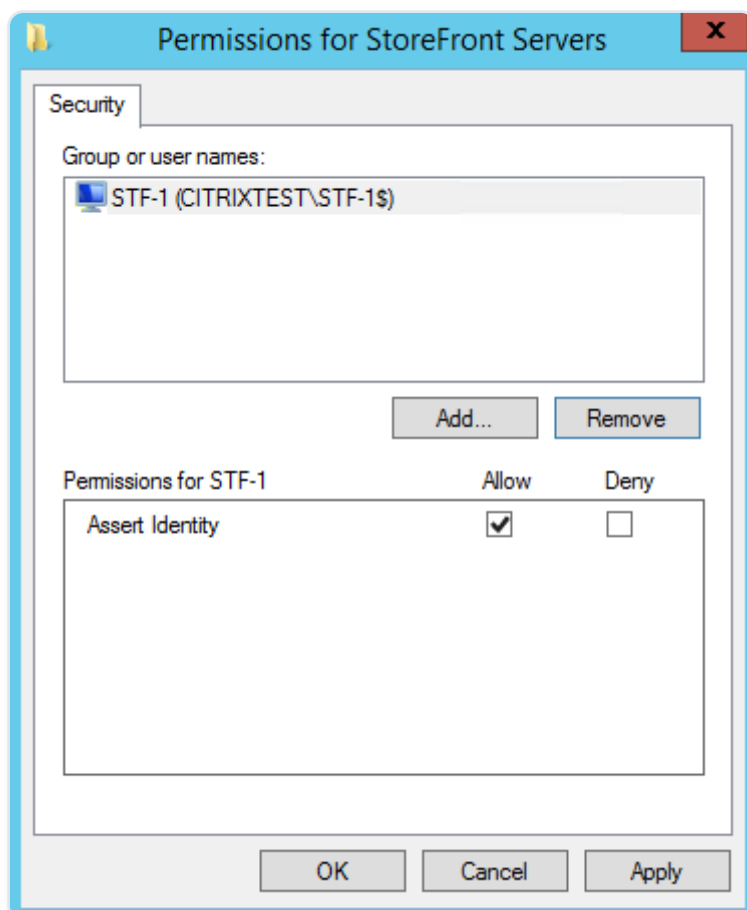
アクセスコントロール: ユーザーのログオンまたは再接続のために証明書を要求することを承認された、信頼されているStoreFrontサーバーマシンのリスト。これらのすべての権限に対して、個々のADオブジェクトまたはグループを追加できます。

重要:

アクセス制御の設定はセキュリティ上重要であり、慎重に管理する必要があります。

注:

FASサーバーをCitrix Cloudでのみ使用している場合、アクセス制御を構成する必要はありません。Citrix Cloudでルールが使用される場合、StoreFrontのアクセス許可は無視されます。Citrix CloudとオンプレミスのStoreFront展開の両方で同じルールを使用できます。オンプレミスのStoreFrontでルールが使用される場合、StoreFrontのアクセス許可は引き続き適用されます。デフォルトの権限（「Assert Identity」が許可されている）はすべてを拒否します。そのため、StoreFrontサーバーを明示的に許可する必要があります。

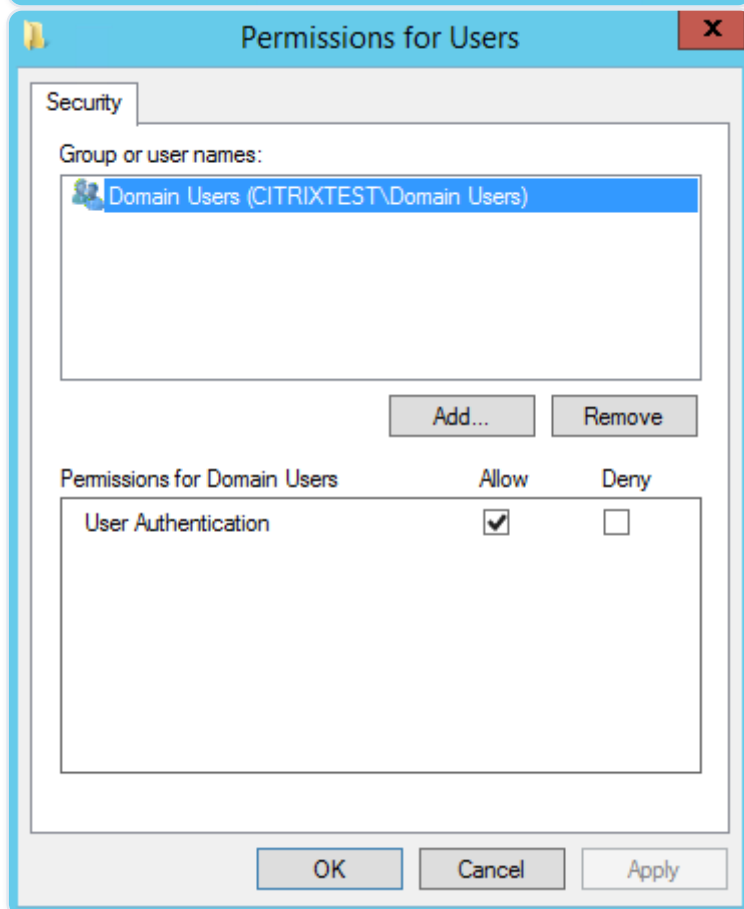
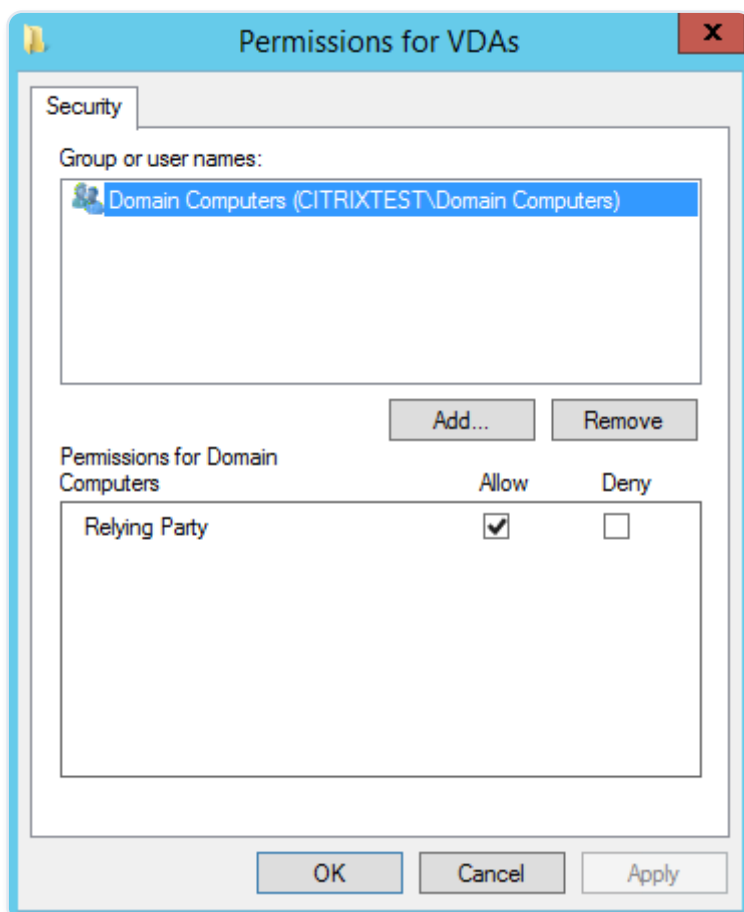


制限: FASを使用してユーザーをログオンできるVDAマシンのリストと、FASを介して証明書を発行できるユーザーのリスト。

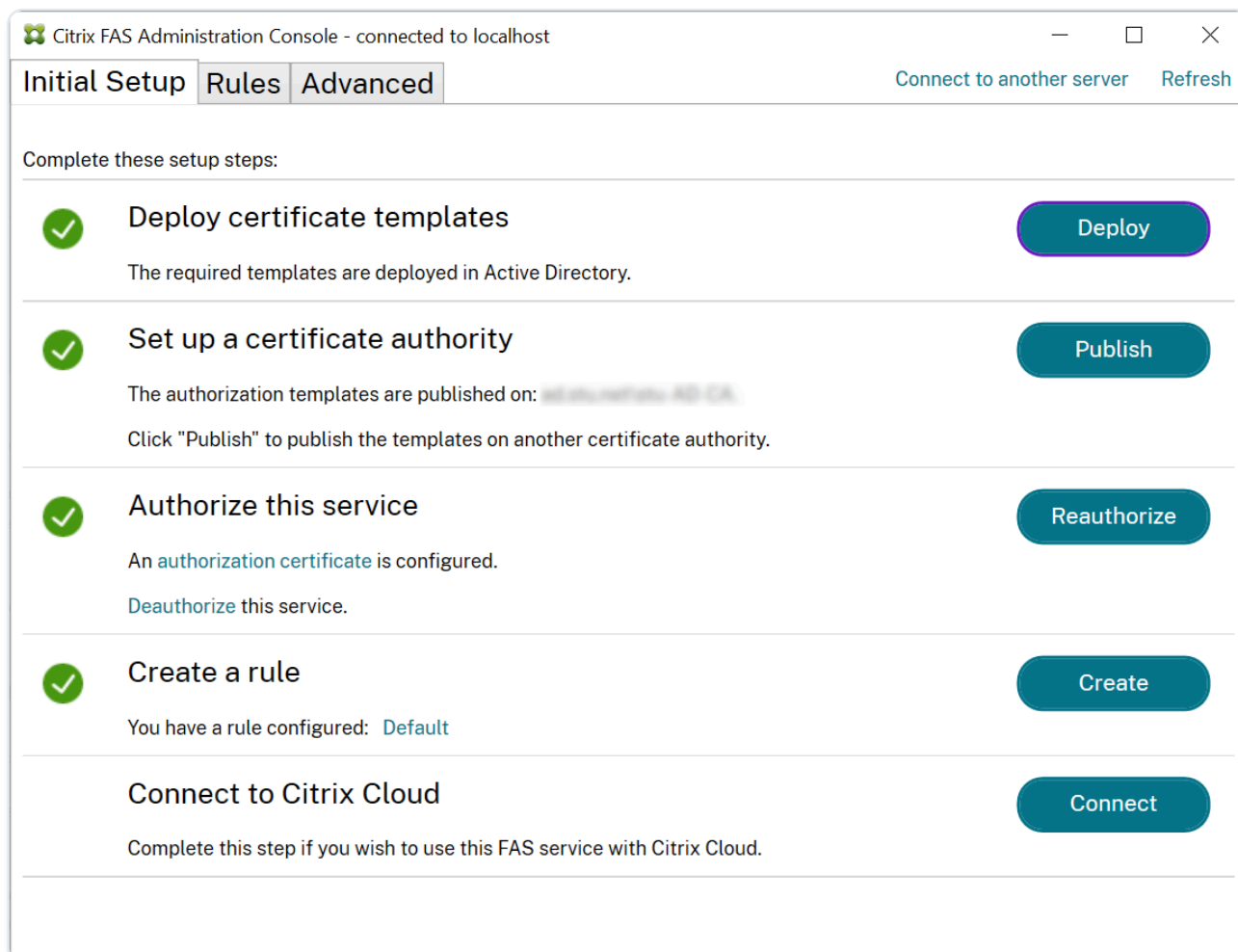
- **VDA権限の管理**では、FASを使用してユーザーをログオンできるVDAを指定できます。VDAのリストはデフォルトでDomain Computersです。
- **ユーザー権限の管理**では、FASを使用してVDAにサインインできるユーザーを指定できます。ユーザーのリストはデフォルトでDomain Usersです。

注:

FASサーバーのドメインがVDAおよびユーザーのドメインと異なる場合、デフォルトの制限を変更する必要があります。



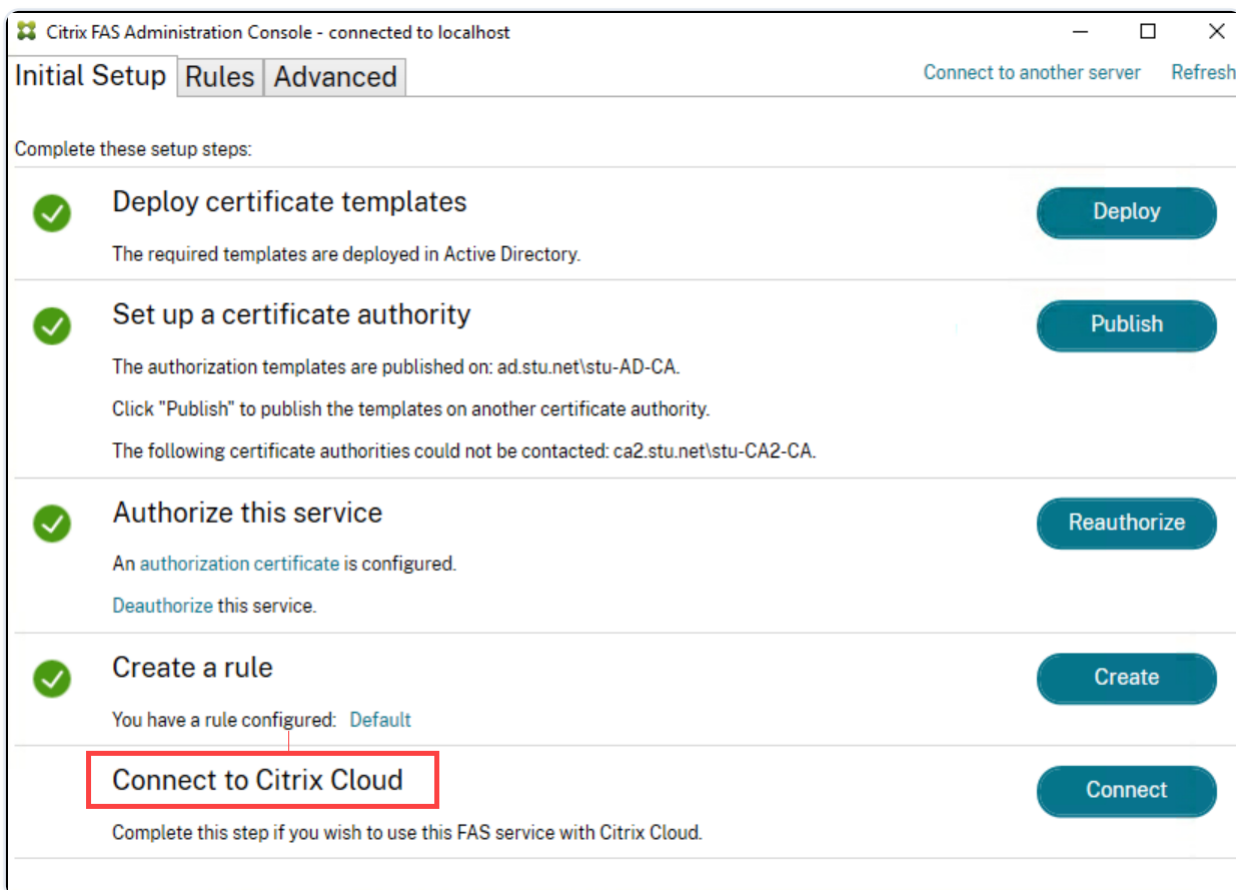
クラウド規則: Citrix WorkspaceからIDアサーションが受信されたときにルールが適用されるかどうかを示します。Citrix Cloudに接続するときに、Citrix Cloudで使用するルールを選択します。Citrix Cloudに接続した後、**Connect to Citrix Cloud**セクションのリンクからルールを変更することもできます。



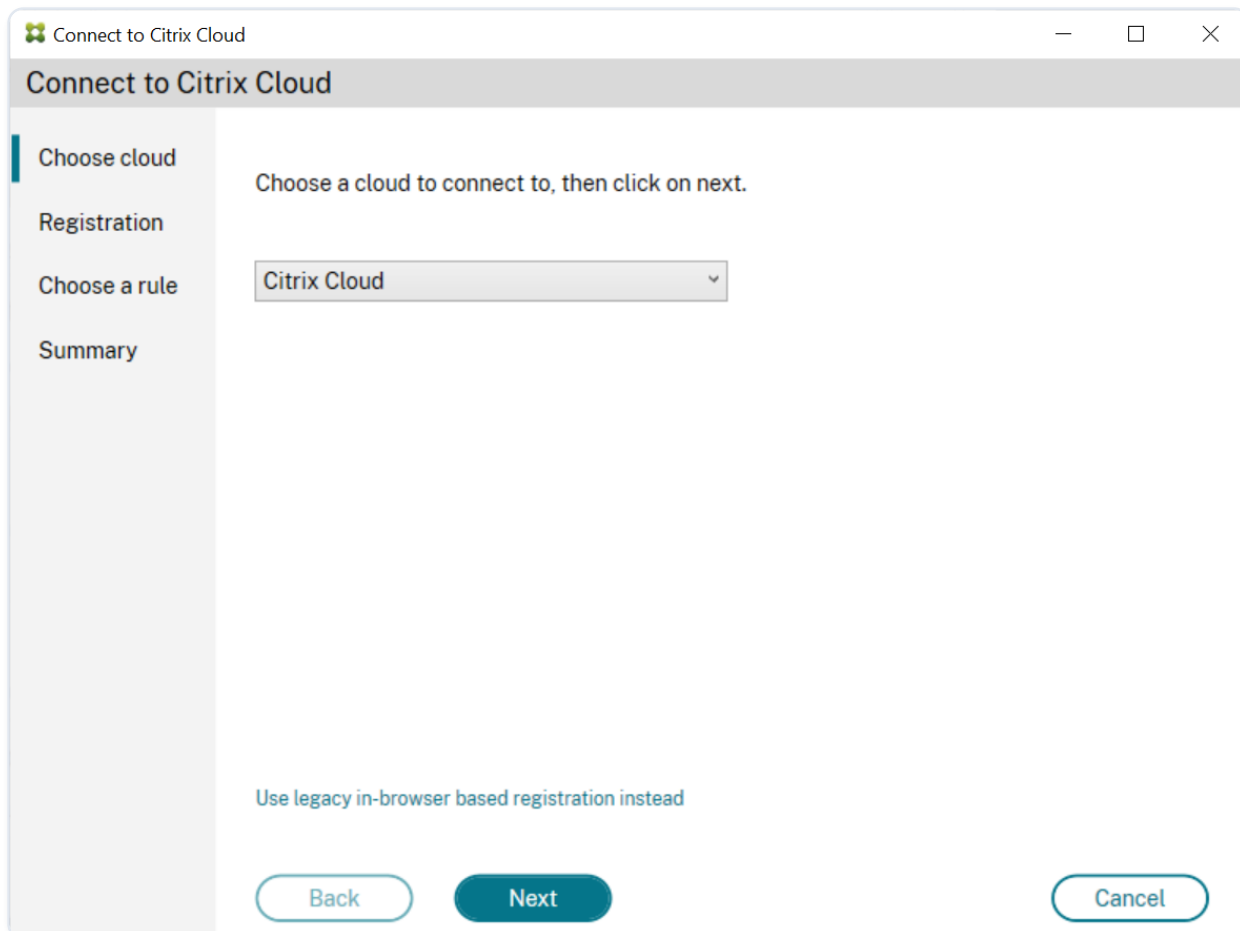
Citrix Cloud に接続する

FAS サーバーを Citrix Workspace を使用して Citrix Cloud に接続できます。この[Citrix Workspace の記事](#)を参照してください。

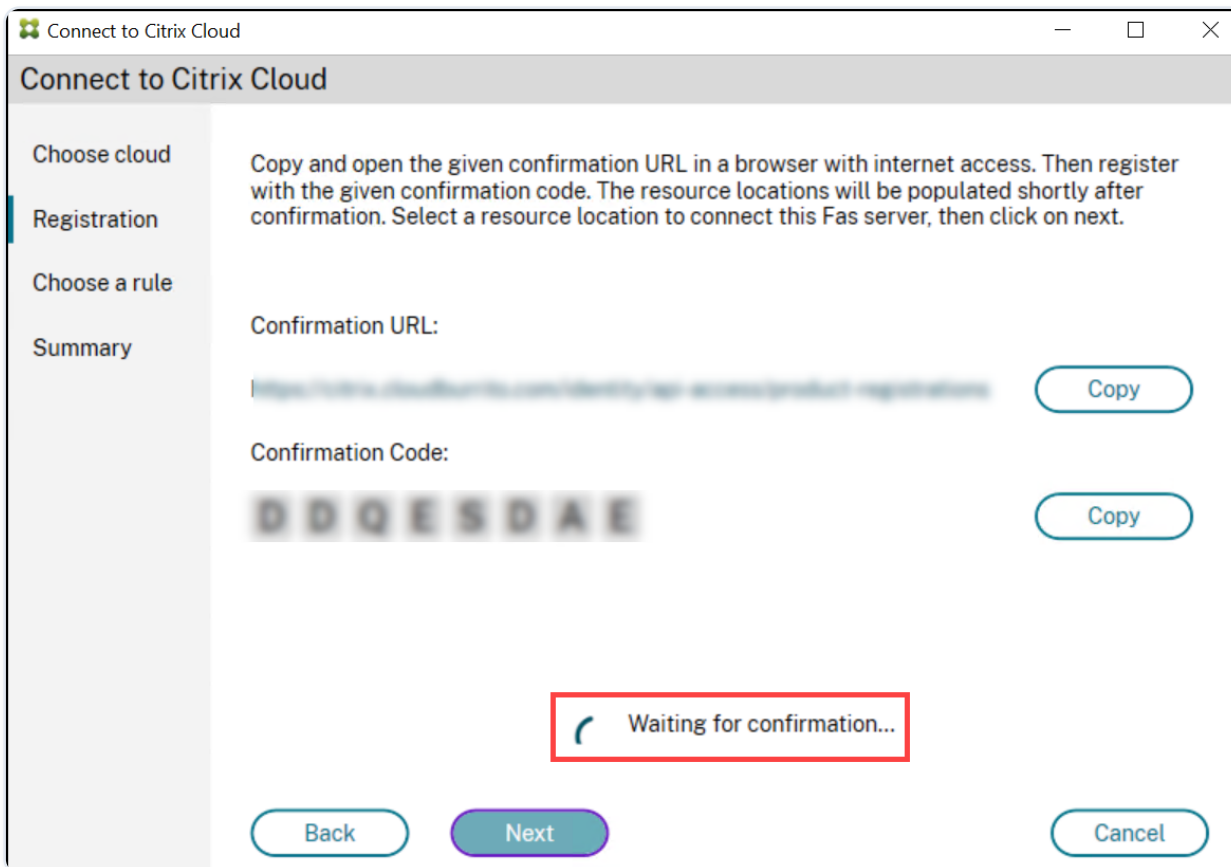
1. Initial Setup タブの をクリックします。



2. 接続するクラウドを選択し、をクリックします。



3. ウィンドウに一意的登録コードが表示されます。このコードは Citrix Cloud で承認する必要があります。詳しくは、[オンプレミス製品を Citrix Cloud に登録する](#)を参照してください。



4. 登録コードが検証されたら、ドロップダウンリストから必要な を選択します。

Connect to Citrix Cloud

Choose cloud

Registration

Choose a rule

Summary

Copy and open the given confirmation URL in a browser with internet access. Then register with the given confirmation code. The resource locations will be populated shortly after confirmation. Select a resource location to connect this Fas server, then click on next.

Confirmation URL:

[https://www.citrix.com/identity/api/.../product/registration](#) Copy

Confirmation Code:

7 8 5 5 2 8 8 8 Copy

Resource location:

My Resource Location

Back Next Cancel

5. 該当する場合は顧客アカウントを選択し、FAS サーバーを接続するリソースの場所を選択します。をクリックし、確認ウィンドウを閉じます。
6. セクションで、既存のルールを使用するか、ルールを作成します。をクリックします。

Connect to Citrix Cloud

Connect to Citrix Cloud

Choose cloud

Registration

Choose a rule

Summary

Choose a FAS rule to use with Citrix Cloud.

☐ I will configure a rule later
☐ Create a rule when this wizard finishes
☒ Use an existing rule:

☒ Default

The rule you use for Citrix Cloud can also be used with on-premises StoreFront.

Back Next Cancel

7. セクションで、をクリックして Citrix Cloud への接続を完了します。

Connect to Citrix Cloud

Connect to Citrix Cloud

Choose cloud

Registration

Choose a rule

Summary

Summary

Customer: (blurred)

Resource location: (blurred)

Rule: Default

Cloud: Citrix Cloud

Back Finish Cancel

Citrix Cloud は FAS サーバーを登録し、Citrix Cloud アカウントの ページに表示します。

注：

オンプレミスの FAS サーバーは、Citrix Cloud と Citrix Virtual Apps and Desktops へのアクセスを同時に許可するユーザー証明書を発行できます。

Citrix Cloud から切断する

この (</ja-jp/citrix-workspace/workspace-federated-authentication.html>) に記載されているように、Citrix Cloud リソースの場所から FAS サーバーを削除した後、[こちら](#)で [Citrix Cloud から切断する](#) を選択します。

高度な構成

このセクションの記事では、Federated Authentication Service (FAS) の高度な構成と管理に関するガイダンスを提供します。

関連情報

- FAS のインストールと初期設定に関する主要なリファレンスは、[インストールと構成](#) の記事です。
- [展開アーキテクチャ](#) の記事では、主要な FAS アーキテクチャの概要と、より複雑なアーキテクチャに関する他の記事へのリンクを提供します。

FAS V2 チケットिंगとレジストリアドレスリスト

FAS 2511より前は、FASはインデックスバイトで始まる**V1**（バージョン1）形式のチケットを作成していました。VDAは、どのFASサーバーがチケットを発行したかを判断する必要があります。これは、インデックスバイトを使用して、レジストリ内のFASアドレスのリストからFASアドレスを検索することで行われます。

通常、GPOはVDA上のFASアドレスのリストを構成します。Windows VDAでは、アドレスリストのレジストリの場所は

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\Authentication\UserCredentialService\Addresses
```

です。

VDA上のアドレスリストはStoreFront上のアドレスリストと完全に一致している必要があります。そうでない場合、シングルサインオンは失敗します。この要件は、特に複雑な展開を行っているお客様にとって、構成エラーの大きな原因となっていました。

FAS 2511では、**V2**（バージョン2）形式のチケットが導入されました。FASサーバーのアドレス（つまり、FQDNとポート）はチケット自体に書き込まれるため、VDAはレジストリアドレスリストを参照する必要がありません。

互換性

2511以降、FASはデフォルトでV2チケットを生成します。V2チケットは、すべてのWindowsおよびLinux VDAバージョンと互換性があります。

バージョン2511より前のVDAは、前のセクションで説明したように、インデックスバイトを使用してレジストリアドレスリストを参照し続けます。

2511以降のWindowsおよびLinux VDAのみがV2チケットを解析できるため、レジストリアドレスリストは必要ありません。

V2チケットはStoreFrontのどのバージョンとも互換性があり、StoreFrontのアップグレードは不要です。

V2チケットで問題が発生した場合は、このPowerShellコマンドを使用してFASがV1チケットを生成するように構成できます。

```
Set-FasServer -Address localhost -TicketVersion 1
```

V2チケットの生成に戻すには、このPowerShellコマンドを使用します。

```
Set-FasServer -Address localhost -TicketVersion 2
```

VDAが認識するFASチケットバージョン

VDA 2511以降のみがV2チケットを解析できます。以前のバージョンでは、V2チケットはV1チケットであるかのように扱われます。

VDAがV2チケットバージョンを認識しているかどうかを確認するには、FASサーバーのイベントログを調べます。

FASとVDAが2511以降の場合、VDAの起動中に以下のようなイベントログエントリが表示されます。イベントは、FASサーバーの**Windowsログ > アプリケーションログ**にあります。

Level: Information

Source: Citrix.Authentication.FederatedAuthenticationService

EventId: 204

```
Text: [S204] Relying party [VDA machine name] accessing the Logon Provider
for [User UPN] in role: [FAS Role] [Operation: XXXX] as authorized by
[StoreFront machine name]. Caller ticket version: 2. [correlation: XXXX]
```

このイベントでは、呼び出し元チケットのバージョンは2です。これは、VDAをレジストリFASアドレスリストで構成する必要がないことを示しています。

逆に、VDAがV2チケットをサポートしていない場合、イベントログエントリの呼び出し元チケットのバージョンは1になります。

```
Level: Information
```

```
Source: Citrix.Authentication.FederatedAuthenticationService
```

```
EventId: 204
```

```
Text: [S204] Relying party [VDA machine name] accessing the Logon Provider
for [User UPN] in role: [FAS Role] [Operation: XXXX] as authorized by
[StoreFront machine name]. Caller ticket version: 1. [correlation: XXXX]
```

StoreFrontでFAS V2チケットを構成する

FASチケットはStoreFrontにとって不透明であるため、どのバージョンのStoreFrontでも使用でき、特別な構成は必要ありません。

StoreFrontでのFASサーバーアドレスの構成は、GPOを使用して提供されるレジストリアドレスリストを引き続き使用します。

Citrix Cloud WorkspaceでFAS V2チケットを構成する

FASがCitrix Cloudに接続されている場合、FASは、そのアドレスが自身のレジストリアドレスリストに存在することを要求します。この動作はV1チケットをサポートするためです。見つからない場合、FAS管理コンソールは警告を表示し、FASはCitrix Cloud Workspaceの起動にシングルサインオンを提供しません。

ただし、展開全体がV2チケットを使用している場合（つまり、FASサーバーとVDAが2511以降の場合）、FASサーバー上のレジストリアドレスリストは不要です。

クラウド接続されたFASがレジストリアドレスリストを要求しないようにするには、次のPowerShellを使用できます。

```
Set-FasCloudConfig -Address localhost -SkipGpoCheck $true
```

その他のPowerShellの変更点

上記のコマンドに加えて、FAS 2511のPowerShellで以下の変更が行われました。

FASサーバーのFQDNとポートを表示する

次のPowerShellコマンドは、FASサーバーのFQDNとリスニングポートを返します。これは、V2チケットにエンコードされるFASアドレス情報です。

```
Get-FasServer -Address localhost
```

コマンドレットのアドレスパラメーター

Prior to 2511, any Address parameter of a FAS PowerShell command (other than "localhost") was checked against the FAS server's registry address list. To change this behavior, it was necessary to use the following command:

```
Set-FasAdministrationPolicy -CheckAddressAgainstGpo $false
```

From 2511 onwards, FAS PowerShell commands don't check the Address parameter against the address list. To revert to the previous behavior, run the following PowerShell command:

```
Set-FasAdministrationPolicy -CheckAddressAgainstGpo $true
```

テナント顧客向けにフェデレーション認証サービスを有効にする

この記事では、マルチテナントのマネージドサービスプロバイダー (MSP) 環境でフェデレーション認証サービス (FAS) を有効にする手順について説明します。詳細については、「[リファレンスアーキテクチャ: Citrix Service Provider DaaS](#)」を参照してください。

前提条件

- Citrix Cloud のドメインとリソースの場所に管理者アクセス権があること。詳細については、「[管理者権限の変更](#)」を参照してください。

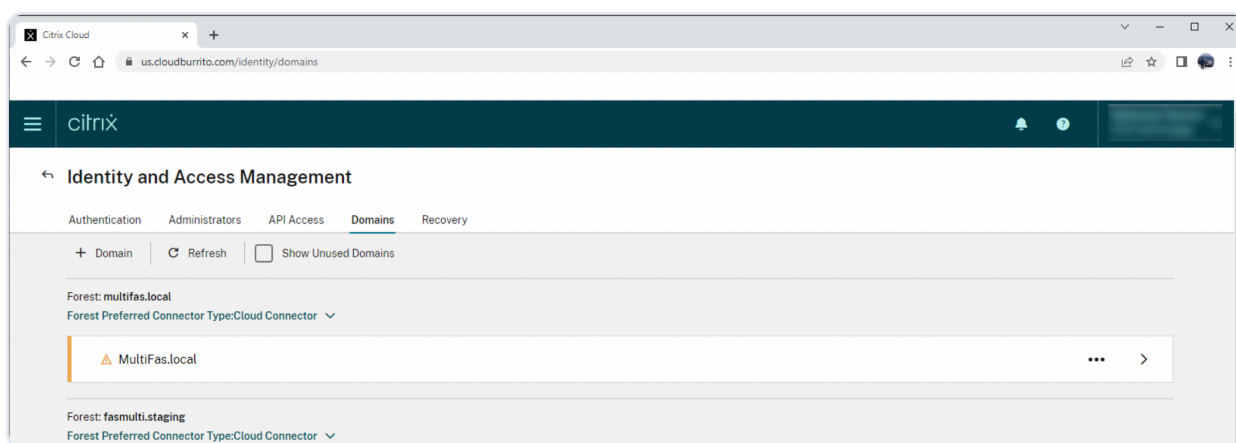
- テナントとMSPの関係を設定済みであること。詳細については、「Citrix Service Provider 向け Citrix DaaS」を参照してください。

MSP顧客の構成

1. Cloud Connector を使用して、Active Directory ドメインを Citrix Cloud で利用できるようにします。

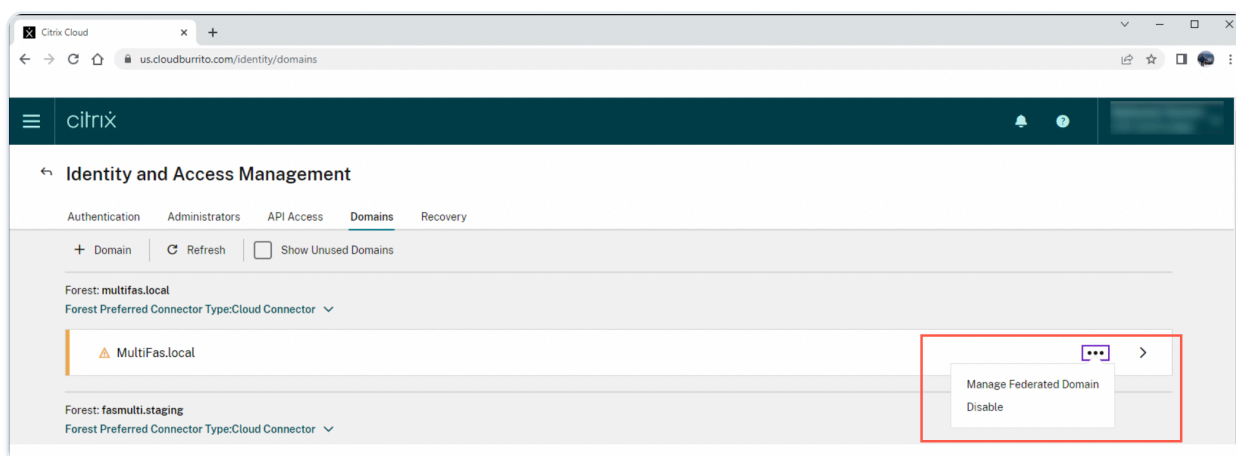
Cloud Connector をインストールして、オンプレミスインフラストラクチャを Citrix Cloud に接続します。

オンプレミスのドメインコントローラーに関連付けられているドメインが、> の下に表示されていることを確認します。



2. ドメインをテナントにフェデレーションします。

ドメインを選択し、ドロップダウンメニュー (...) をクリックして、 をクリックします。



テナントを見つけて をクリックします。次に をクリックします。

Add or remove customers to create a federated domain

1 available customers [Add all](#)

0 federated customers [Remove all](#)

Search... Q

Search... Q

FAS Tenant1 with service profile. +

Cancel Apply

3. 関連付けられているドメインがテナントに存在することを確認します。

この手順はオプションです。テナント顧客のコンソールにサインインし、>の下にドメインがリストされていることを確認します。

関連付けられているドメインがテナントに存在することを確認します(/en-us/federated-authentication-service/2511/media/fas-verify-domains.png)

MSP 顧客に戻ります。

4. FAS サーバーをインストールし、Citrix Cloud に登録します。

テナントの Citrix Virtual Apps and Desktops リソースが配置されている Active Directory (AD) フォレストに FAS をインストールします。FAS をその AD フォレストに関連付けられているクラウドのリソースの場所に接続します。FAS サーバーをインストールするには、「[インストールと構成](#)」を参照してください。

5. テナント顧客を構成する

テナント顧客向けに FAS を有効にする

- ID プロバイダー (IdP) を構成する

テナント顧客に切り替えます。 > に移動します。 IdP に接続し、AD が IdP と同期されていることを確認します。

- テナント向けに FAS を有効にする

> に移動します。設定した認証を選択し、FAS を有効にします。

FAS テナントを有効にする(/en-us/federated-authentication-service//current-release/media/fas-enable-tenant.png)

既知の問題

テナントのフェデレーションドメインを削除する前に MSP ドメインを削除すると、既知の問題が発生します。テナント向けに FAS を有効にすることはできますが、MSP にドメインが存在しなくなるため、FAS は失敗します。

Azure Active Directory シングルサインオン

注:

2023年7月以降、MicrosoftはAzure Active Directory (Azure AD) をMicrosoft Entra IDに名称変更しました。このドキュメントでは、Azure Active Directory、Azure AD、またはAADへの言及はすべてMicrosoft Entra IDを指します。

Citrix Federated Authentication Service (FAS) は、ドメイン参加済みVirtual Delivery Agent (VDA) へのシングルサインオン (SSO) を提供します。FASは、VDAにユーザー証明書を提供することでSSOを実現します。この証明書をVDAは使用して、ユーザーをActive Directory (AD) に対して認証します。VDAセッションにサインオンすると、再認証なしでADリソースにアクセスできます。

ADとMicrosoft Entra ID間で同期を行い、ユーザーとコンピューターの両方にハイブリッドIDを作成するMicrosoft Entra ID (ME-ID) の実装は一般的です。この記事では、FASを使用している場合に、VDAセッション内からMicrosoft Entra IDへのSSOを実現するために必要な追加構成について説明します。これにより、ユーザーは再認証なしでMicrosoft Entra IDで保護されたアプリケーションにアクセスできるようになります。

注:

- Microsoft Entra IDのSSOを使用するために、FASに特別な構成は必要ありません。
- FASのセッション内証明書は必要ありません。
- FASのどのバージョンでも使用できます。
- FASをサポートするVDAのどのバージョンでも使用できます。

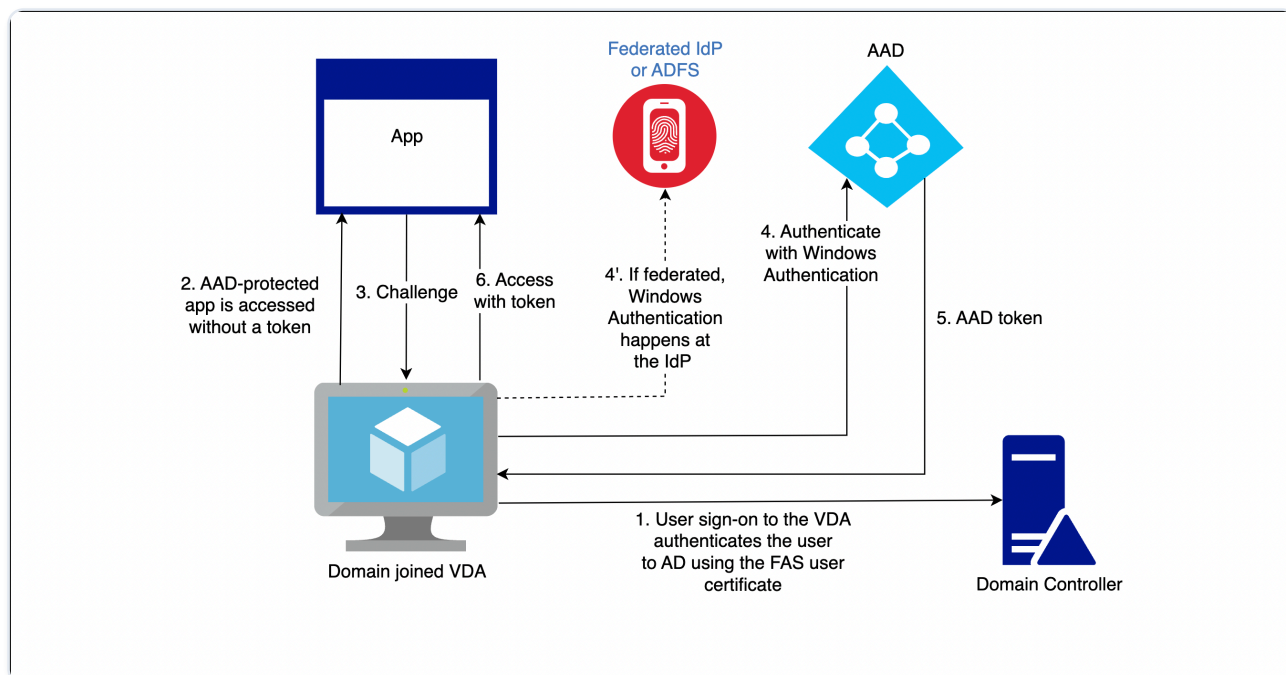
Microsoft Entra ID SSOの技術は、次の表にまとめられています。

ME-ID認証タイプ	VDAはドメイン参加済み	VDAはハイブリッド参加済み
マネージド	ME-ID シームレス SSO を使用する	ME-ID 証明書ベース認証を使用する
Active Directory フェデレーション サービス (ADFS) にフェデレーション済み	ADFS で Windows 認証を有効にする	WS-Trust の <i>certificatemixed</i> エンドポイントが有効になっていることを確認する
サードパーティの ID プロバイダーにフェデレーション済み	サードパーティ ソリューションを使用する	サードパーティ ソリューションを使用する

- マネージド Microsoft Entra ID ドメインとは、ユーザー認証が Microsoft Entra ID で行われるドメインであり、ネイティブ Microsoft Entra ID 認証と呼ばれることもあります。
- フェデレーション Microsoft Entra ID ドメインとは、Microsoft Entra ID が認証を別の場所にリダイレクトするように構成されているドメインです。たとえば、ADFS やサードパーティの ID プロバイダーなどです。
- ハイブリッド参加 VDA は、AD 参加済みであり、Microsoft Entra ID 参加済みです。

ドメイン参加済み VDA

ドメイン参加済み VDA の場合、Windows 認証 (従来は統合 Windows 認証または Kerberos と呼ばれていました) を使用して Microsoft Entra ID への SSO を実現します。Microsoft Entra ID への認証は、ユーザーが VDA セッション内から Microsoft Entra ID で保護されたアプリケーションにアクセスしたときに発生します。次の図は、認証プロセスを大まかに示しています。



正確な詳細は、Microsoft Entra ID ドメインがマネージドであるかフェデレーションであるかによって異なります。

管理されたMicrosoft Entra IDドメインのセットアップについては、[Seamless single sign-on](#)を参照してください。

ADFSにフェデレーションされたMicrosoft Entra IDドメインの場合、ADFSサーバーでWindows認証を有効にします。

サードパーティのIDプロバイダーにフェデレーションされたMicrosoft Entra IDドメインの場合、同様のソリューションが存在します。詳細については、IDプロバイダーにお問い合わせください。

注：

ドメイン参加済みVDAに記載されているソリューションを、ハイブリッド参加済みVDAにも使用できます。ただし、FASを使用している場合、Microsoft Entra IDプライマリ更新トークン（PRT）は生成されません。

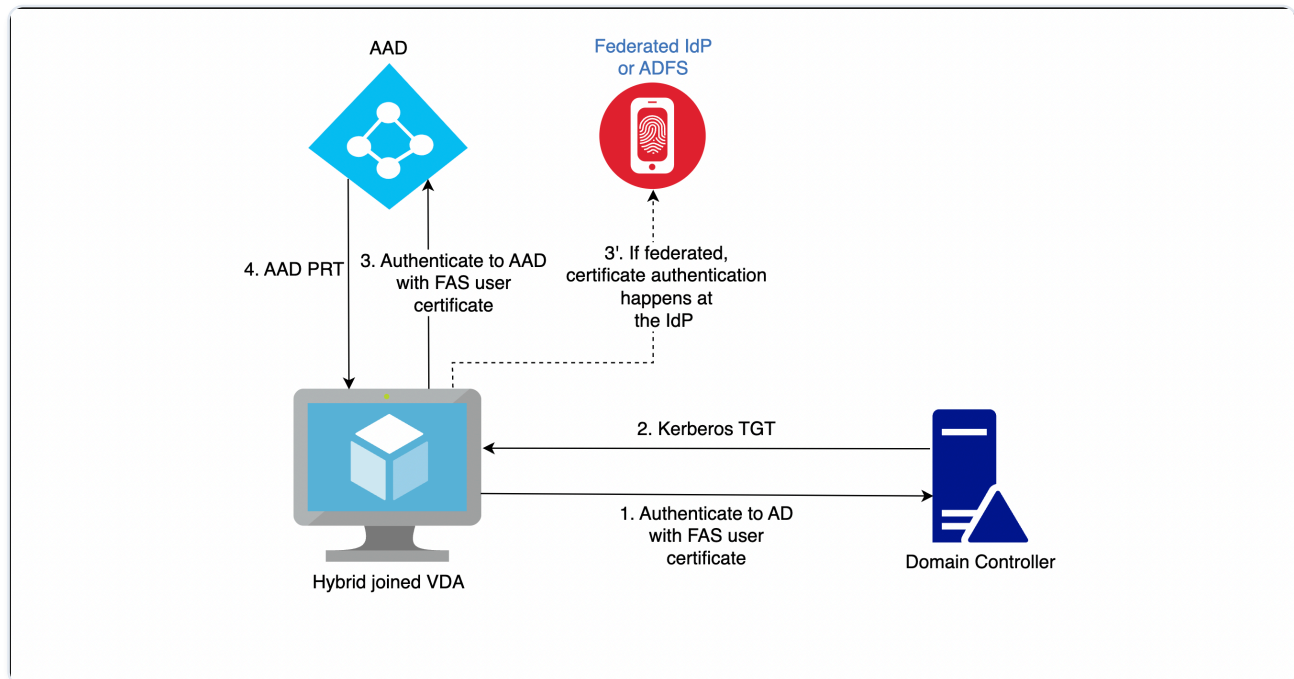
ハイブリッド参加済みVDA

ハイブリッド参加済みVDAは、ADとMicrosoft Entra IDに同時に参加しています。ユーザーがVDAにサインインすると、次のアーティファクトが作成されます。

- ADリソースへの認証のためのKerberosチケット保証チケット（TGT）
- Microsoft Entra IDリソースへの認証のためのプライマリ更新トークン（PRT）

PRTには、ユーザーとコンピューターの両方に関する情報が含まれています。この情報は、必要に応じてMicrosoft Entra ID条件付きアクセス ポリシーで使用されます。

FASはVDAに証明書を提供することでユーザーを認証するため、PRTはMicrosoft Entra IDの証明書ベース認証が実装されている場合にのみ作成できます。次の図は、認証プロセスを大まかに示しています。



正確な詳細は、Microsoft Entra IDドメインが管理されているかフェデレーションされているかによって異なります。

管理されたMicrosoft Entra IDドメインの場合、Microsoft Entra ID CBAを構成します。詳細については、[Azure AD 証明書ベースの認証の概要](#)を参照してください。VDAはMicrosoft Entra ID CBAを使用して、ユーザーのFAS証明書でMicrosoft Entra IDにユーザーを認証します。

注：

The Microsoft documentation describes sign in with a smart card certificate, but the underlying technique applies when signing in with a FAS user certificate.

For an Microsoft Entra ID domain federated to ADFS, the VDA uses the ADFS server's WS-Trust *certificatemixed* endpoint to authenticate the user to Microsoft Entra ID with the user's FAS certificate. This endpoint is enabled by default.

サードパーティのIDプロバイダーにフェデレーションされたMicrosoft Entra ID ドメインの場合、同様のソリューションが存在する可能性があります。IDプロバイダーは、WS-Trust

certificatemixed エンドポイントを実装する必要があります。詳細については、IDプロバイダーにお問い合わせください。

認証局の構成

この記事では、Federated Authentication Service (FAS) を証明機関 (CA) サーバーと統合するための高度な構成について説明します。これらの構成のほとんどは、FAS 管理コンソールではサポートされていません。手順では、FAS が提供する PowerShell API を使用します。この記事のいずれかの手順を実行する前に、PowerShell の基本的な知識が必要です。

FAS で使用する複数の CA サーバーをセットアップする

ルールを作成または編集する際に、FAS 管理コンソールを使用して複数の CA で FAS を構成できます。

Name	Status
☒ ad-01u-net-01u-AD-CA	Template available
☒ ad-01u-net-01u-CA2-CA	Template available

選択するすべての CA は、Citrix_SmartcardLogon 証明書テンプレート（またはルールで選択したテンプレート）を公開している必要があります。

使用したい CA のいずれかが目的のテンプレートを公開していない場合は、その CA に対して **認証局をセットアップする** の手順を実行してください。

注：

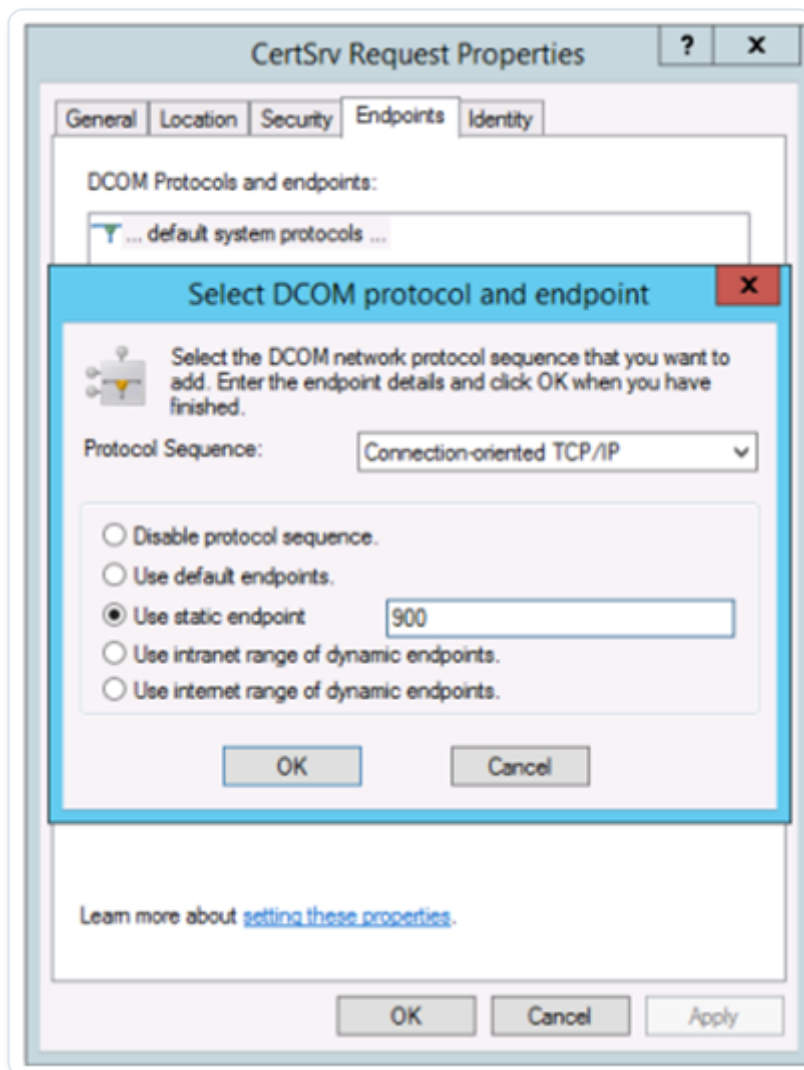
すべてのCAに対して、[このサービスを承認する](#)の手順を実行する必要はありません。この手順で構成された承認証明書は、どのCAでも使用できるためです。

予期される動作の変更

FASサーバーを複数のCAサーバーで構成すると、ユーザー証明書の生成は構成されているすべてのCAサーバーに分散されます。また、構成されているCAサーバーのいずれかが失敗した場合、FASサーバーは別の利用可能なCAサーバーに切り替わります。

TCP アクセス用に Microsoft 証明機関を構成する

FAS は Microsoft CA に DCOM を使用してアクセスします。DCOM はポート 135 を使用して、サービスがリッスンしているポートを検出します。デフォルトでは、リッスンポートは動的に割り当てられます。これは、ファイアウォールセキュリティを実装する際に複雑さを生じさせる可能性があります。そのため、Microsoft は静的ポートを構成する機能を提供しています。Microsoft CA で静的ポートを構成するには、**Start > Run > dcomcnfg.exe** を選択して **DCOM configuration** パネルを開きます。**Computers > My computer > DCOM Config** を展開して CertSrv Request ノードを表示します。次に、CertSrv Request DCOM アプリケーションのプロパティを編集します。



Endpoints を変更して静的エンドポイントを選択し、TCPポート番号 (上記のグラフィックでは 900) を指定します。

この例では、ファイアウォールはポート135とポート900を許可する必要があります。

変更を適用するには、Microsoft証明機関を再起動します。

DCOMはRPCポート135を使用してネゴシエーション段階を持つため、FASサーバー（または証明機関を使用する他のマシン）を設定する必要はありません。クライアントがDCOMを使用する必要がある場合、サーバー上のDCOM RPCサービスに接続し、特定のDCOMサーバーへのアクセスを要求します。これにより、ポート900（この例では）が開かれ、DCOMサーバーはクライアントにそのポートへの接続を指示します。

ユーザー証明書を事前生成する

FASサーバー内でユーザー証明書が事前生成されると、ユーザーのログオン時間が大幅に改善されます。以下のセクションでは、単一または複数のFASサーバーでこれを実現する方法について説明します。

Active Directoryユーザーのリストを取得する

以下の例に示すように、ADをクエリし、ユーザーのリストをファイル（たとえば、.csvファイル）に保存することで、証明書の生成を改善できます。

```
Import-Module ActiveDirectory

$searchbase = "cn=users,dc=bvt,dc=local" # AD User Base to Look for Users,
leave it blank to search all

$filename = "user_list.csv" # Filename to save

if ($searchbase -ne ""){

    Get-ADUser -Filter {(UserPrincipalName -ne "null") -and (Enabled -eq
"true")}} -SearchBase $searchbase -Properties UserPrincipalName | Select
UserPrincipalName | Export-Csv -NoTypeInfoInformation -Encoding utf8
-delimiter "," $filename

} else {

    Get-ADUser -Filter {(UserPrincipalName -ne "null") -and (Enabled -eq
"true")}} -Properties UserPrincipalName | Select UserPrincipalName |
Export-Csv -NoTypeInfoInformation -Encoding utf8 -delimiter "," $filename

}
```

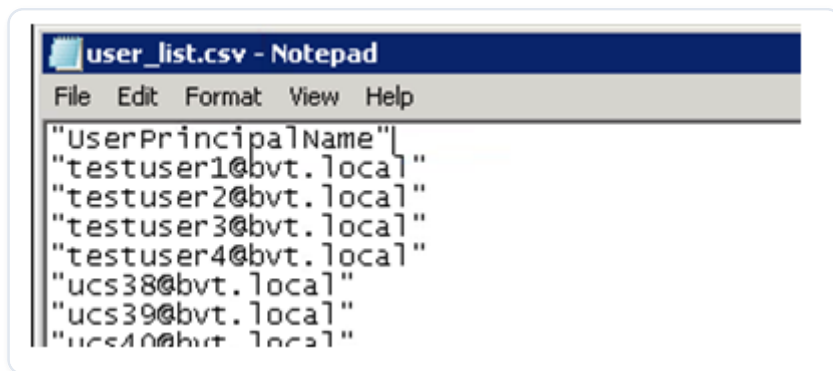
`Get-ADUser` は、ユーザーのリストをクエリするための標準的なコマンドレットです。上記の例には、`UserPrincipalName`を持ち、アカウントステータスが「enabled」のユーザーのみをリストするためのフィルター引数が含まれています。

`SearchBase`引数は、ADのどの部分でユーザーを検索するかを絞り込みます。AD内のすべてのユーザーを含めたい場合は、これを省略できます。

注:

このクエリは多数のユーザーを返す可能性があります。

CSVは次のようになります。



FASサーバー

以下のPowerShellスクリプトは、以前に生成されたユーザーリストを受け取り、ユーザー証明書
のリストを作成します。

```
Add-PSSnapin Citrix.A*

$csv = "user_list.csv"

$rule = "default" # rule/role in your admin console

$users = Import-Csv -encoding utf8 $csv

foreach ( $user in $users )
{
    $server = Get-FasServerForUser -UserPrincipalName
    $user.UserPrincipalName

    if( $server.Server -ne $NULL) {

        New-FasUserCertificate -Address $server.Server -UserPrincipalName
        $user.UserPrincipalName -CertificateDefinition $rule"_Definition" -Rule
        $rule

    }

    if( $server.Failover -ne $NULL) {

        New-FasUserCertificate -Address $server.Failover
        -UserPrincipalName $user.UserPrincipalName -CertificateDefinition
```

```
$rule"_Definition" -Rule $rule  
  
}  
  
}
```

FASサーバーが複数ある場合、特定のユーザーの証明書は2回生成されます。1つはメインサーバーで、もう1つはフェイルオーバーサーバーで生成されます。

この前のスクリプトは、「default」という名前のルールに対応しています。異なるルール名（例：「hello」）を使用している場合は、スクリプト内の `$rule` 変数を変更してください。



Citrix FAS Administration Console - connected to localhost

Initial Setup Rules Advanced [Connect to...](#)

A rule defines a smartcard-class certificate that signs users into a Citrix environment.

[+ Create rule](#)

Rule Name	Summary
Default	
hello	

Rule name: hello

Status: OK

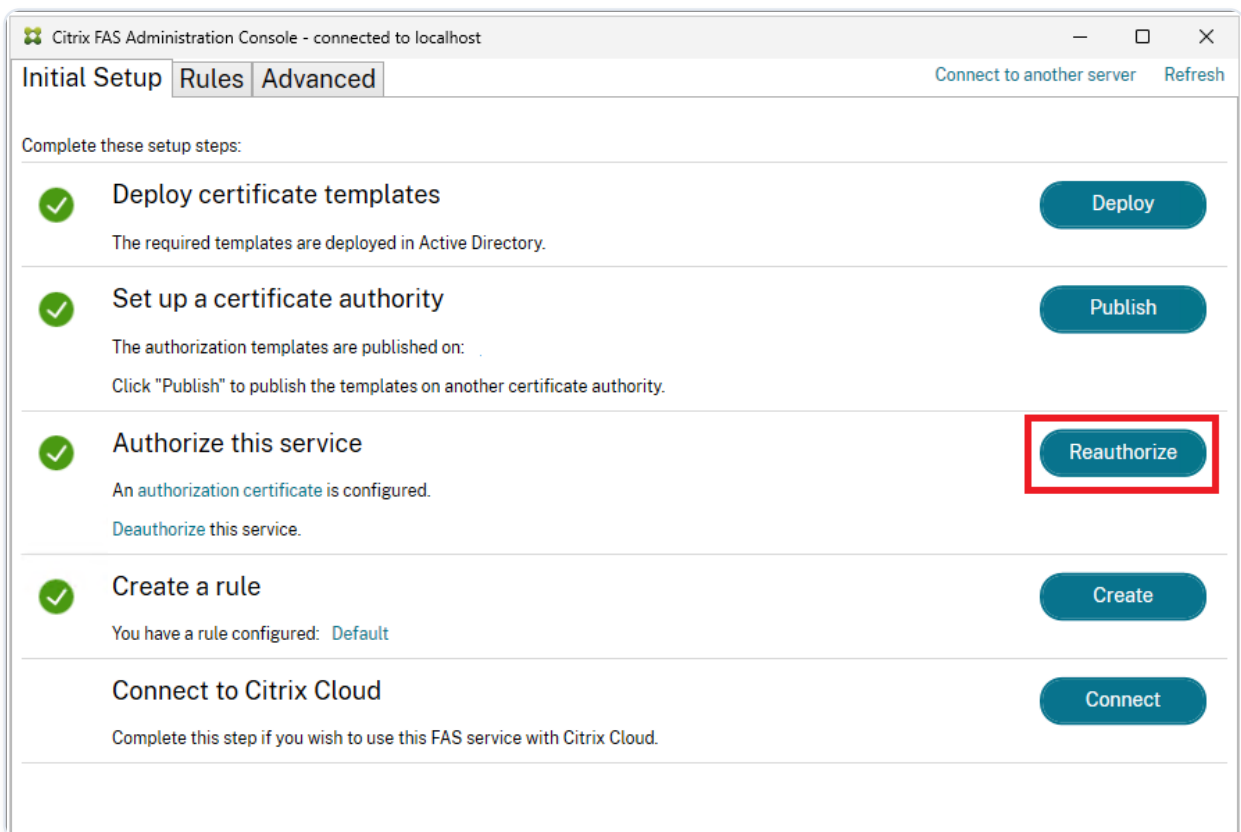
Template: Citrix_SmartcardLogon

FAS承認証明書の更新

FASユーザーに影響を与えることなく、FAS承認証明書を更新できます。

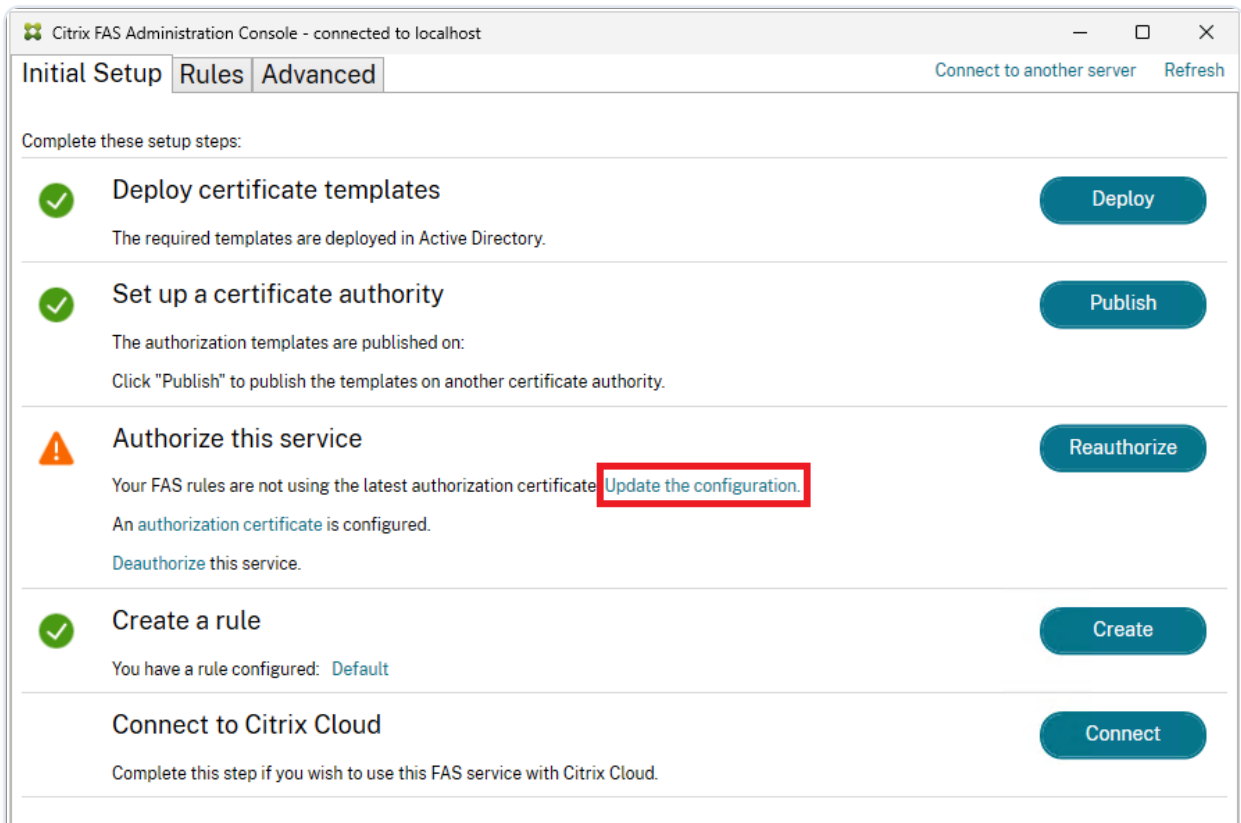
FAS管理コンソールの使用

- 新しいFAS承認証明書要求を生成するには、**再承認**をクリックします。



CAで要求を手動で承認する必要があります。詳細については、[フェデレーション認証サービスを承認する](#)を参照してください。

- 新しい承認証明書が生成されると、FASはそれがまだルールに関連付けられていないことを示します。新しい承認証明書をルールに関連付けるには、**構成を更新**をクリックします。



PowerShellの使用

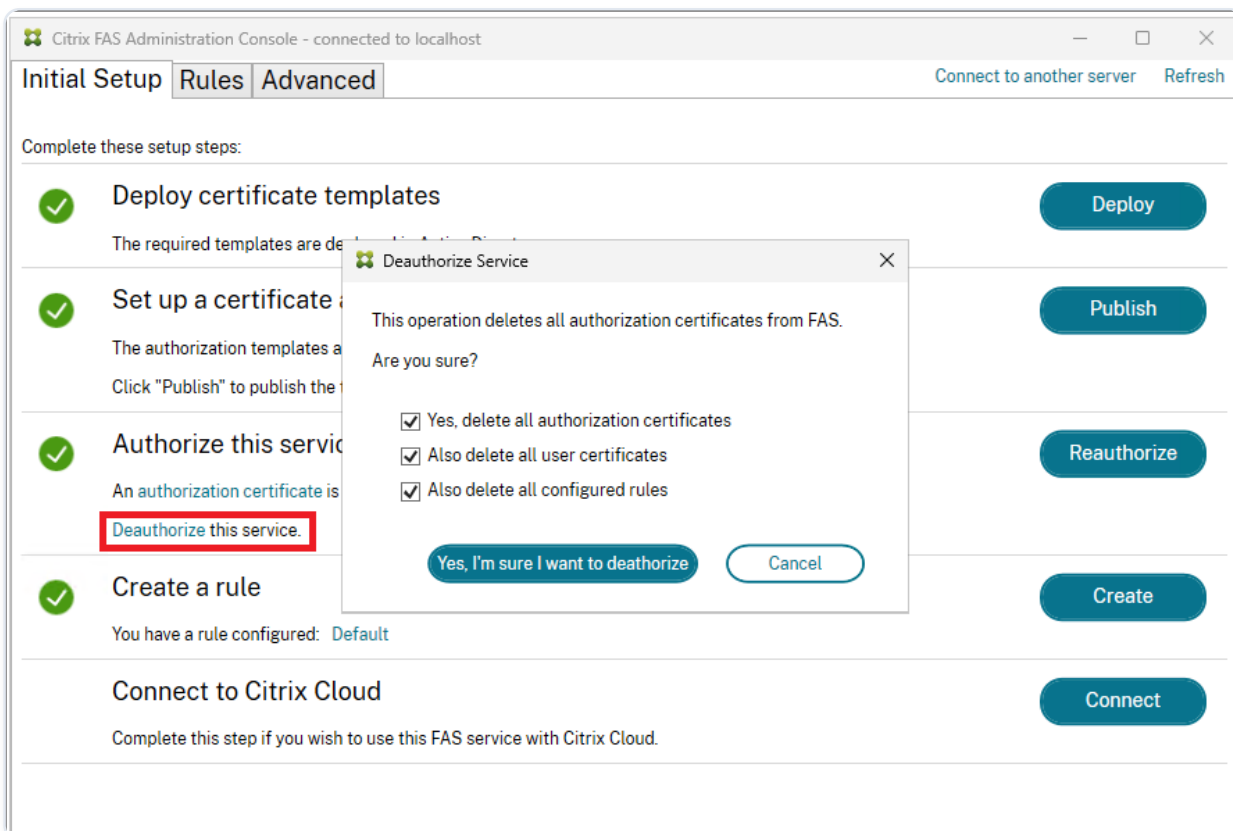
次のシーケンスを完了します。

1. 承認証明書を作成します: `New-FasAuthorizationCertificate`
2. 新しい承認証明書のGUIDを、`Get-FasAuthorizationCertificate` によって返されるとおりにメモします。
3. 新しい承認証明書を交換します: `Set-FasCertificateDefinition - AuthorizationCertificate <GUID>`
4. 古い承認証明書を削除します: `Remove-FasAuthorizationCertificate`。ユーザーのアクティビティが中断されないように、`DeleteUserCerts $false option` を使用してください。

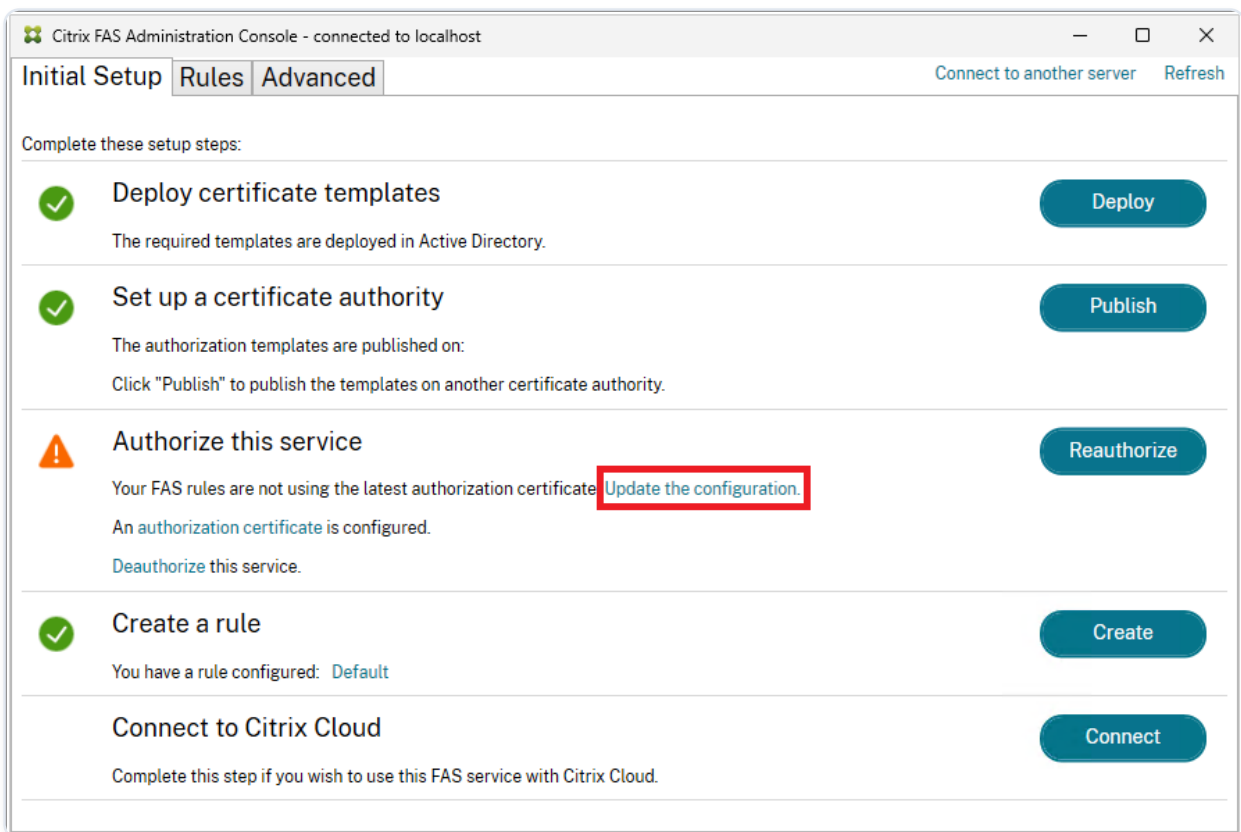
FASの認証解除とFAS証明書の削除

FAS管理コンソールの使用

- **Deauthorize** リンクをクリックして、承認証明書を削除します。すべてのユーザー証明書とすべてのルールを削除できます（ただし、証明書をクリアするために必須ではありません）。



- ルールを削除しない場合、後でFASを承認すると警告が表示されます。



この警告は、承認証明書がまだルールに関連付けられていないことを示しています。**Update the configuration**をクリックして、新しい承認証明書をルールに関連付けます。

PowerShellの使用

承認証明書とユーザー証明書を削除するには、次のPowerShellコマンドを使用します。

```
$AuthCert = Get-FasAuthorizationCertificate -Address localhost  
  
Remove-FasAuthorizationCertificate -Address localhost -Id $AuthCert.Id
```

注：

`Get-FasAuthorizationCertificate` は、承認証明書と保留中の承認証明書要求のリストを返します。`Remove-FasAuthorizationCertificate` に進む前に、`$AuthCert` の値を検査してください。

`DeleteUserCerts` パラメーターをfalseに設定すると、承認証明書を削除し、ユーザー証明書を保持できます。

```
Remove-FasAuthorizationCertificate -Address localhost -Id $AuthCert.Id  
-DeleteUserCerts $false
```

残りのユーザー証明書は、VDAサインインおよびセッション内証明書としてFASで引き続き使用できます。これは、FAS承認を更新する際に役立ちます。詳細については、「[Renew FAS authorization certificate](#)」を参照してください。

- ユーザー証明書は次のように削除できます。

```
Remove-FasUserCertificate -Address localhost
```

このコマンドは、FASサーバーからすべてのユーザー証明書を削除します。このコマンドには、削除される証明書のセットをフィルター処理するオプションがあります。

「

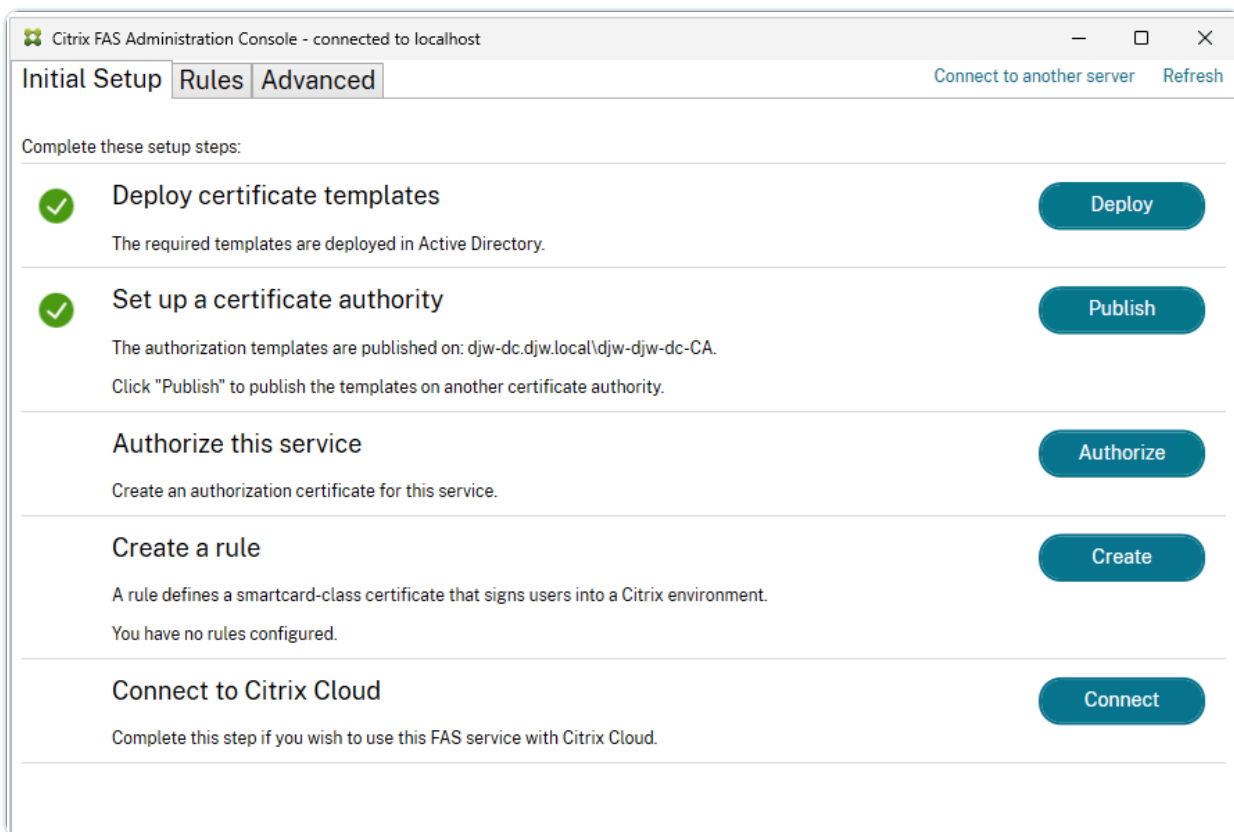
注：

FASが内部ストレージから承認またはユーザー証明書を削除すると、関連するキーペアも削除されます。

オフライン承認

FAS承認証明書は、PowerShellを使用してオフラインで要求できます。これは、証明機関がオンライン証明書署名要求を通じて承認証明書を発行することを望まない組織に適しています。

1. 管理コンソールを使用して初期FAS構成を行う際は、最初の2つの手順のみを完了してください。「[証明書テンプレートの展開](#)」と「[証明機関のセットアップ](#)」です。



2. FASサーバーで次のPowerShellコマンドレットをロードします。

```
Add-PSSnapin Citrix.Authentication.FederatedAuthenticationService.V1`
```

3. FASサーバーで次のPowerShellコマンドレットを入力して、キーペアを生成し、証明書署名要求を作成します。

```
$AuthCertRequest = New-FasAuthorizationCertificateRequest -Address  
localhost $AuthCertRequest
```

これにより、次の結果が得られます。

結果(/en-us/federated-authentication-service/2511/media/result-new-fas-auth-cert.png)

「

注：

生成されたキーペアのプロパティは、FAS承認キー構成によって決定されます。詳細については、「プライベートキーの保護」(</ja-jp/federated-authentication-service/2511/config-manage/private-key-protection.html>)を参照してください。

4. 証明書要求をディスクにコピーします。

```
`$AuthCertRequest.CertificateRequest > c:\temp\authcert.csr`
```

5. 証明書要求ファイル（この例ではauthcert.csr）を証明機関に提示し、要求を承認して、証明書応答を取得します。

次の5つの手順は、Microsoft Enterprise証明機関の使用に特有のものです。他のCAについては、CAベンダーに問い合わせて支援を受けてください。

- 証明機関サーバーで、証明書テンプレートMMCスナップインを追加します。
「Citrix_RegistrationAuthority_ManualAuthorization」テンプレートを右クリックし、「**テンプレートの複製**」を選択します。「**全般**」タブを選択します。名前と有効期間を変更します。この例では、名前はOffline_RAで、有効期間は2年です。

Properties of New Template

Subject Name	Server	Issuance Requirements
Superseded Templates		Extensions
Security		
Compatibility	General	Request Handling
Cryptography	Key Attestation	

Template display name:
Offline_RA

Template name:
Offline_RA

Validity period: 2 years Renewal period: 0 days

☐ Publish certificate in Active Directory
☐ Do not automatically reenroll if a duplicate certificate exists in Active Directory

OK Cancel Apply Help

- 認証局サーバーで、認証局MMCスナップインを追加します。証明書テンプレートを右クリックします。新規を選択し、発行する証明書テンプレートをクリックします。作成したテンプレートを選択します。
- FASサーバーのPowerShellコマンドプロンプトに以下を入力して、証明書署名要求を認証局に送信します。

```
certreq -submit -attrib "certificatetemplate:<certificate template from step 5a>" <certificate request file from step 4>
```

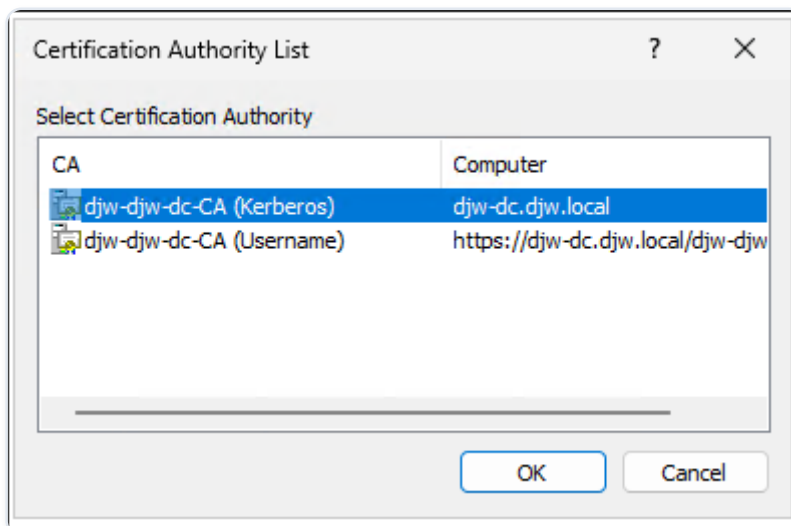
例：

```
certreq -submit -attrib "certificatetemplate:Offline_RA" C:\temp\authcert.csr
```

前のコマンドを実行すると、次の結果が表示されます。

```
PS C:\> certreq -submit -attrib "certificatetemplate:Offline_RA" C:\temp\authcert.csr
Active Directory Enrollment Policy
{3C06E1D3-4E2D-4B8B-94FA-C254192D09C6}
ldap:
```

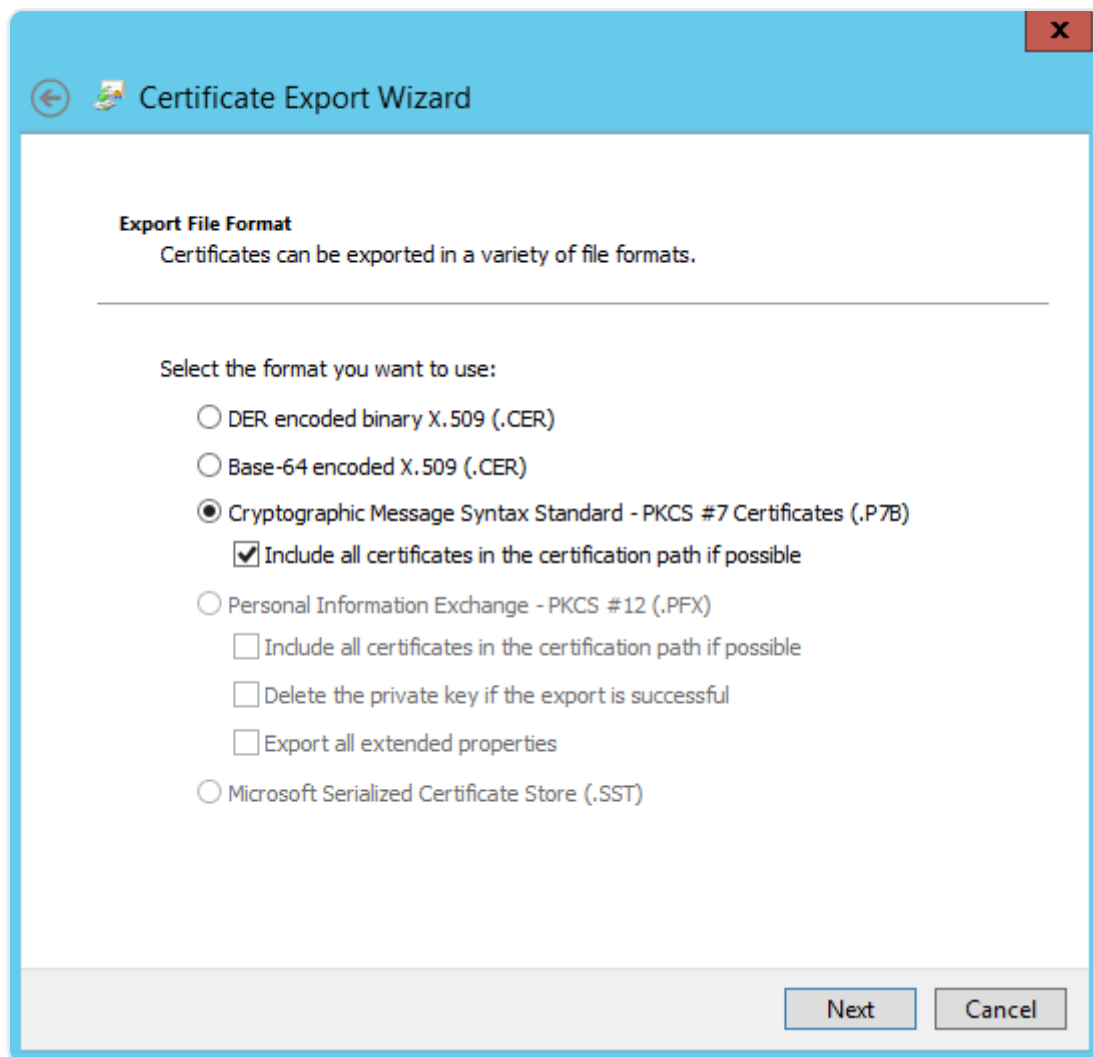
この時点で、認証局リストウィンドウが表示される場合があります。この例の認証局では、DCOM（上）とHTTP（下）の両方の登録が有効になっています。利用可能な場合は**DCOM**を選択し、**OK**をクリックします。



認証局が指定されると、コマンドが完了し、RequestIdが表示されます。

```
PS C:\> certreq -submit -attrib "certificatetemplate:Offline_RA" C:\temp\authcert.csr
Active Directory Enrollment Policy
{3C06E1D3-4E2D-4B8B-94FA-C254192D09C6}
ldap:
RequestId: 358
RequestId: "358"
Certificate request is pending: Taken Under Submission (0)
PS C:\> |
```

- 認証局サーバーで、認証局MMCスナップインの**保留中の要求**をクリックします。要求IDを見つけます。次に、要求を右クリックし、**発行**を選択します。
- **発行された証明書**ノードを選択します。発行された証明書を見つけます（要求IDが一致する必要があります）。証明書をダブルクリックして開きます。**詳細**タブを選択します。**ファイルにコピー**をクリックします。**証明書のエクスポートウィザード**が起動します。次へをクリックします。ファイル形式について次のオプションを選択します。



形式は**暗号メッセージ構文標準 – PKCS #7 証明書 (.P7B)**であり、**可能であれば、証明のパスにあるすべての証明書を含める**が選択されている必要があります。

6. エクスポートされた証明書ファイルをFASサーバーにコピーします。
7. FASサーバーで次のPowerShellコマンドレットを入力して、登録機関証明書をFASサーバーにインポートします。

```
Import-FasAuthorizationCertificateResponse -Address localhost -Id  
$AuthCertRequest.Id -Pkcs7CertificateFile <Certificate file from step  
6>
```

例:

```
Import-FasAuthorizationCertificateResponse -Address localhost -Id  
$AuthCertRequest.Id -Pkcs7CertificateFile C:\temp\response.p7b
```

このコマンドを実行すると、次の結果が得られます:

FAS承認証明書のインポート応答(/en-us/federated-authentication-service/2511/media/import-fas-auth-cert-response.png)

8. FAS管理コンソールを確認します。FASが承認されていることが表示されているはずです。

サービスを承認(/en-us/federated-authentication-service/2511/media/fas-admin-console-authorize-service.png)

注:

このサービスを承認ステップの横に緑色のチェックマークが表示されます。

9. ルールを作成して構成を続行します。詳細については、[ルールを構成する](#)を参照してください。

関連情報

- [インストールと構成](#)の記事は、FASのインストールと構成に関する主要なリファレンスです。
- 一般的なフェデレーション認証サービス展開は、[展開アーキテクチャ](#)の記事にまとめられています。
- その他のハウツー記事は、[高度な構成](#)の記事で紹介されています。

秘密鍵の保護

はじめに

FAS証明書は、FASサーバー上の組み込みデータベースに保存されます。FAS証明書に関連付けられた秘密鍵は、FASサーバーのネットワークサービスアカウントの下に保存されます。デフォルトでは、キーはエクスポート不可の2048ビットRSAであり、Microsoft Software Key Storage Providerで作成および保存されます。

FAS PowerShellコマンド[PowerShellコマンドレット](#)を使用すると、秘密鍵のプロパティと保存場所を変更できます。

注:

FASの構成と証明書は、FASサーバーにローカルに保存されます。データはFASサーバー間で共有されません。

Citrix Virtual Apps and Desktops 2411より前のFASリリースでは、秘密鍵のプロパティは `%programfiles%\Citrix\Federated Authentication`

`Service\Citrix.Authentication.FederatedAuthenticationService.exe.config` にあるXMLファイルを編集することで構成されていました。これはPowerShellコマンドに置き換えられました。PowerShellコマンドは、より柔軟性があり、FASサーバーを再起動せずに適用できます。さらに、XMLファイルの設定とは異なり、PowerShellを使用して行われた構成は、FASサーバーがアップグレードされても保持されます。したがって、以下の設定に対するXMLファイルを使用した構成はサポートされなくなりました。

- `Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.KeyProtection`
- `Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.ProviderLegacyCsp`
- `Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.ProviderName`
- `Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.ProviderType`
- `Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.KeyLength`

「Citrix Virtual Apps and Desktops™ 2411より前のFASバージョンからのアップグレード」のセクションを参照してください。

FAS証明書とテンプレートに関する情報

FASが保持する証明書には2種類あります。通常1つのインスタンスである承認証明書と、ユーザー証明書です。

注:

FAS承認証明書は、**登録機関**または**要求エージェント (RA)** 証明書とも呼ばれることがあります。

FASは、証明書を要求する際に証明書テンプレートを使用します。これについては、次のセクションで説明します。FASは証明書要求でテンプレート名を指定しますが、テンプレートの内容は読み取りません。したがって、テンプレートの設定を変更しても、FASが行う証明書要求には影響しません。テンプレートの特定のプロパティを変更すると、CAによって生成される証明書に影響します。たとえば、テンプレートを使用して有効期間を変更できます。

FAS承認証明書

この証明書は、FASを構成するときに作成されます。FAS管理コンソールの**承認**または**再承認**ボタンを使用して、新しい承認証明書を要求できます。

PowerShellコマンドを使用することも可能で、これにより柔軟性が向上します。

- `New-FasAuthorizationCertificate` : このコマンドはFAS管理コンソールと同様に動作しますが、承認プロセスで使用する証明書テンプレートを指定できる点が異なります。
- `New-FasAuthorizationCertificateRequest` : このコマンドは、承認証明書のオフライン要求を作成します。 [オフライン承認](#)。

承認証明書は、FASが登録機関として機能し、ユーザーに代わって証明書を要求するため、RA証明書とも呼ばれることがあります。この証明書には、拡張キー使用法証明書要求エージェントがあり、FASユーザー証明書を要求する際の承認資格情報として使用できます。

デフォルトでは、承認プロセスは次のテンプレートを使用します。

- `Citrix_RegistrationAuthority_ManualAuthorization` : このテンプレートを使用して作成された証明書は一時的で短命であり、承認プロセスをブートストラップするために使用されます。
- `Citrix_RegistrationAuthority` : このテンプレートを使用して作成された証明書は有効期間が長く、FASサーバーによって保存されます。

FASを承認すると、次の手順が実行されます。

1. FASはキーペアを作成し、キーペアの公開鍵とテンプレート `Citrix_RegistrationAuthority_ManualAuthorization` を指定して、**証明書署名要求 (CSR)** をCAに送信します。
2. テンプレートの発行要件では、CSRはCA管理者によって手動で承認される必要があると指定されています。
3. CA管理者がCSRを承認すると、CAはFASが取得する証明書を作成します。この証明書の有効期間は1日と短く、次のステップでのみ使用されます。使用されると、FASはその証明書とキーペアを破棄します。
4. FASは別のキーペアを作成し、2番目のCSRをCAに送信します。このCSRでは、このキーペアの公開鍵とテンプレート `Citrix_RegistrationAuthority` を指定します。この要求は、前のステップで取得した証明書によって承認され、署名されます。
5. CAは自動的に証明書を発行し、FASはその証明書を取得します。これにより、FASは**承認済み**の状態になります。デフォルトでは、この承認証明書の有効期間は2年間です。

前述のキーペアの作成に使用された設定は、次のPowerShellコマンドを使用して表示できます。

```
Get-FasKeyConfig -Address localhost -CertificateType ra
```

FASユーザー証明書

FASは、ユーザーをVDAにサインインさせるためにユーザー証明書を作成します。

FASがユーザー証明書を作成する際には、次の手順が実行されます。

- FASはキーペアを作成し、CSRをCAに送信します。このCSRでは、キーペアの公開鍵、ユーザーのID、およびデフォルトでテンプレート `Citrix_SmartcardLogon` を指定します（使用されるテンプレートは構成可能です）。
- CSRはFAS承認証明書を使用して署名されます。
- `Citrix_SmartcardLogon` テンプレートには発行要件 `Application Policy: Certificate Request Agent` があります。この属性はFAS承認証明書に存在するため、CAはユーザー証明書を自動的に発行します。
- FASは証明書を取得し、FASサーバー上の組み込みデータベースに保存します。
- デフォルトでは、証明書の有効期間は1週間です。

その後、ユーザー証明書はユーザーをサインインさせるためにVDAで利用可能になります。

前述のキーペアの作成に使用された設定は、次のPowerShellコマンドを使用して表示できます。

```
Get-FasKeyConfig -Address localhost -CertificateType user
```

秘密鍵の保存オプション

FASは、キーペアを3つのカテゴリのストレージに作成および保存するように構成できます。

- **ソフトウェア:** 通常、**Microsoft Software Key Storage Provider**を使用します。これはソフトウェアのみで保護され、データはディスクに保存されます。
- **Trusted Platform Module (TPM):** TPMは、コンピューター上の物理ハードウェアであるか、ハイパーバイザーによって提供される仮想TPMである場合があります。
- **Hardware Security Module (HSM):** これは、暗号化キーを安全に保存するように設計されたハードウェア周辺機器またはネットワークデバイスです。

注:

考慮すべきトレードオフがあります。ハードウェアストレージはより安全である可能性がありますが、特に多数のユーザー証明書キーペアを作成および保存する場合、パフォーマンスが低下することがよくあります。

FAS承認証明書に関連付けられた秘密鍵は特に機密性が高く、証明書のポリシーにより、秘密鍵を所有する者は誰でも、任意のユーザーの証明書要求を承認できるためです。結果として、この鍵を制御する者は誰でも、任意のユーザーとして環境に接続できます。

注:

Microsoft CAは、証明書を発行できるユーザーのセットを含め、FAS承認証明書の権限を制限するように構成できます。詳細については、「[委任された登録エージェント](#)」を参照してください。

このため、FASでは、承認証明書とユーザー証明書の秘密鍵プロパティを個別に構成できます。一般的な構成をいくつか示します。

承認証明書キー	ユーザー証明書キー	コメント
ソフトウェア	ソフトウェア	デフォルト構成
TPM	ソフトウェア	承認証明書にはハードウェア保護があります
HSM	HSM	すべての証明書にはハードウェア保護があります

注:

ハードウェアTPMはユーザーキーには推奨されません。承認証明書キーにのみTPMを使用してください。仮想化環境でFASサーバーを実行する予定がある場合は、ハイパーバイザーベンダーにTPM仮想化がサポートされているか確認してください。

キー構成PowerShellコマンド

秘密キーの構成に関連するコマンドは次のとおりです。

- `Get-FasKeyConfig`
- `Set-FasKeyConfig`
- `Reset-FasKeyConfig`
- `Test-FasKeyConfig`

詳細については、[PowerShell コマンドレット](#)を参照してください。

承認証明書とユーザー証明書のキー構成は独立しており、`CertificateType` 引数で指定されます。例えば、承認証明書 (RA 証明書) を要求する際に使用される秘密鍵構成を取得するには、次のようにします。

```
Get-FasKeyConfig -Address localhost -CertificateType ra
```

ユーザー証明書を要求する際に使用される秘密鍵構成を取得するには、次のようにします。

```
Get-FasKeyConfig -Address localhost -CertificateType user
```

Set-FasKeyConfig と **Get-FasKeyConfig** を使用して、以下の秘密鍵プロパティを設定および検査できます。

プロパティ	既定値	コメント
長さ	2048	ビット単位のキー長。Microsoft テンプレート GUI では、暗号化タブで*最小*キーサイズが指定されていることに注意してください。FAS で構成されたキー長がテンプレートで指定された最小キーサイズよりも小さい場合、CSR は CA によって拒否されます。 RSAキーの場合、長さは1024ビット、2048ビット、または4096ビットにできます。 ECCキーの場合、長さは256ビット、384ビット、または521ビットにできます。
エクスポート可能	偽	プライベートキーをそのプロバイダーからエクスポートできるかどうか。

プロパティ	既定値	コメント
プレフィックス	なし	FASによって生成されるプライベートキーの識別子に追加するプレフィックスを指定します。生成される識別子は、プレフィックスとGUIDで構成されます。例: <code>MyPrefix70277985-6908-4C6F-BE59-B08691456804</code> 。
楕円曲線	偽	trueの場合、ECCキーペアが生成され、それ以外の場合はRSAキーペアが生成されます。
キー記憶域プロバイダー (KSP)	真	trueの場合、FASは最新のWindows CNG APIを使用し、 Provider プロパティでKSPを指定する必要があります。 falseの場合、FASはレガシーCAPI APIを使用し、Providerプロパティで暗号化サービスプロバイダー (CSP) を指定する必要があります。CitrixはKSPの使用を推奨しています。
プロバイダー	Microsoft Software キー ストレージ プロ バイダー	キーペアが作成および保存されるプロバイダーの名前です。このプロパティを変

プロパティ	既定値	コメント
		更して、TPMまたはHSMを指定できます。HSMのKSP (またはCSP) はHSMベンダーによって提供されます。ベンダーは、ソフトウェアのインストール方法とプロバイダーの名前に関する指示を提供します。
CSPタイプ	24	KSPプロパティが falseに設定されている場合にのみ関連します。 Microsoft KeyContainerPermissionAccessEntry.ProviderType Property PROV_RSA_AES 24 を参照してください。CSPを持つHSMを使用しており、HSMベンダーが別途指定しない限り、常に24である必要があります。

さらに、**Set-FasKeyConfig** は、便宜上、以下のスイッチとともに使用できます。

フラグ	説明
-UseDefaultSoftwareProvider	Provider プロパティを Microsoft Software Key Storage Provider に、KSP フィールドを true に設定します。

フラグ	説明
-UseDefaultTpmProvider	Provider プロパティを Microsoft Platform Crypto Provider に、 KSP フィールドを true に設定します。

Microsoft Software Key Storage Provider は、通常、ディスク上にキーを作成および保存するために使用されるプロバイダーです。

Microsoft Platform Crypto Provider は、通常、TPM にキーを作成および保存するために使用されるプロバイダーです。

Get-FasKeyConfig は、どのプロバイダーとアルゴリズムが使用されているかを確認するのに役立つフィールドも提供します。

フィールド	意味
IsDefaultSoftwareProvider	true の場合、プロバイダーが Microsoft Software Key Storage Provider に設定され、 KSP フィールドが true に設定されていることを示します。
IsDefaultTpmProvider	「true」の場合、プロバイダーが「 Microsoft Platform Crypto Provider 」に設定され、「 KSP 」フィールドが「 true 」に設定されていることを示します。
アルゴリズム	「RSA」は、RSAキーが作成されることを示します（「EllipticCurve」プロパティは「false」です）。 「ECC」は、ECCキーが作成されることを示します（「EllipticCurve」プロパティは「true」です）。

Reset-FasKeyConfig を使用して、設定をデフォルトに戻すことができます。

```
Reset-FasKeyConfig -Address localhost -CertificateType ra  
  
Reset-FasKeyConfig -Address localhost -CertificateType user
```

注：

秘密キー構成（`Set-FasKeyConfig` または `Reset-FasKeyConfig` を使用）への変更は、新しく作成された証明書に直ちに適用されます。ただし、異なる構成の既存の承認証明書およびユーザー証明書には影響しません。

既存の証明書は、管理コンソールからFASサービスを非承認にするか、[FASの非承認とFAS証明書の削除](#)のPowerShellコマンドを使用して削除できます。

現在のユーザーキー構成に準拠しないキープール内の事前生成されたキーはすべて破棄されます。

構成シナリオの例

各例では、既存の証明書は構成変更の影響を受けないため、FASサービスを承認する前に、提供されているPowerShellを使用してキー構成を設定してください。

誤ったキー構成の承認証明書またはユーザー証明書が既にある場合は、[FAS証明書の検査とFASの非承認とFAS証明書の削除](#)で削除できます。

FASサーバーがライブ展開にある場合は、構成変更を行う間、メンテナンスモードにすることを検討してください[メンテナンスモード](#)。

例1 - すべてのキーをMicrosoft Software Key Storage Providerに保存する

これはデフォルトであるため、追加の構成は必要ありません。

以前にキー構成を変更した場合は、次のコマンドを使用して **Microsoft Software Key Storage Provider** の使用に戻すことができます。

```
Set-FasKeyConfig -Address localhost -CertificateType ra  
-UseDefaultSoftwareProvider  
  
Set-FasKeyConfig -Address localhost -CertificateType user  
-UseDefaultSoftwareProvider
```

`Reset-FasKeyConfig` を使用して **Microsoft Software Key Storage Provider** に戻し、さらに他のすべてのキー構成設定をデフォルトに復元できます。

例 2 - 認証証明書キーを TPM に保存する

この例では、FAS 認証証明書キーを TPM (物理または仮想) に保存し、ユーザー証明書キーを **Microsoft Software Key Storage Provider** に保存する方法を示します。

FAS は TPM で保護されたキーを持つユーザー証明書を生成できますが、大規模な展開では TPM ハードウェアが遅すぎたり、サイズが制限されたりする可能性があります。

次の PowerShell コマンドを使用します。

```
Set-FasKeyConfig -Address localhost -CertificateType ra  
-UseDefaultTpmProvider  
  
Set-FasKeyConfig -Address localhost -CertificateType user  
-UseDefaultSoftwareProvider
```

例 3 - すべてのキーを HSM に保存する

この例では、HSM を使用して認証証明書とユーザー証明書の両方の秘密キーを保存する方法を示します。この例では、構成済みの HSM を前提としています。HSM にはプロバイダー名があります。たとえば、**HSM Vendor Key Storage Provider** などです。

次の PowerShell コマンドを使用します (例のテキストを HSM のプロバイダーの実際の名前で置き換えてください)。

```
Set-FasKeyConfig -Address localhost -CertificateType ra -Provider "HSM  
Vendor Key Storage Provider"  
  
Set-FasKeyConfig -Address localhost -CertificateType user -Provider "HSM  
Vendor Key Storage Provider"
```

例 4 - 楕円曲線キーを使用する

デフォルトでは、FAS は RSA キーを生成します。この例では、認証証明書とユーザー証明書の両方に楕円曲線 (ECC) キーが構成されています。

この例では、異なるキー長を使用しています。認証証明書は 384 ビットキーで構成され、ユーザー証明書は 256 ビットキーで構成されています。

```
Set-FasKeyConfig -Address localhost -CertificateType ra -EllipticCurve  
$true -Length 384
```

```
Set-FasKeyConfig -Address localhost -CertificateType user -EllipticCurve $true -Length 256
```

この時点では、FAS 証明書テンプレートの最小キーサイズがデフォルトで 1024 ビットに設定されているため、認証およびユーザー証明書要求が CA によって拒否される可能性があります。

したがって、この例では、テンプレートの最小キーサイズを次のように変更する必要があります。

- `Citrix_RegistrationAuthority_ManualAuthorization` and `Citrix_RegistrationAuthority` : 最小キーサイズを 384（またはそれ以下）に変更します。
- `Citrix_SmartcardLogon` : 最小キーサイズを 256（またはそれ以下）に変更します。

テンプレートを編集するには、`mmc.exe` を実行し、**証明書テンプレート**スナップインを追加します。テンプレートを見つけて、そのプロパティを開きます。最小キーサイズの設定は、テンプレートのプロパティの**暗号化**タブにあります。

注：

ECCキーを持つユーザー証明書は、Citrix Virtual Apps and Desktops 2411以降を実行しているWindows VDAでのみサポートされます。ECCキーはLinux VDAではサポートされていません。

秘密キー構成のテスト

`Set-FasKeyConfig` コマンドは一部の検証を行います、無効なキー構成を設定することは依然として可能です。たとえば、HSMのプロバイダー名に誤りがある場合や、指定したキー長がハードウェアでサポートされていない場合があります。

`Test-FasKeyConfig` コマンドが役立ちます。これは現在のキー構成を使用してキーペアの作成を試み、**成功**または**失敗**を報告します。失敗した場合は、その理由が示されます。成功した場合、キーペアは直ちに破棄されます。

次のPowerShellコマンドは、それぞれ認証とユーザーキー構成をテストします。

```
Test-FasKeyConfig -Address localhost -CertificateType ra  
  
Test-FasKeyConfig -Address localhost -CertificateType user
```

FASサーバーを承認し、ルールを作成したら、次のようにユーザー証明書のテストCSRを追加で作成できます。

```
Test-FasCertificateSigningRequest -Address localhost -UserPrincipalName  
user@example.com -Rule default
```

<<mailto:user@example.com>>をActive Directory展開からの実際のUPNに置き換えます。FASルールは通常**default**という名前です。ただし、設定した別のルールをテストしたい場合は、その名前を指定してください。

CSRが成功した場合、FASは結果の証明書を破棄します。

FAS証明書の検査

PowerShellを使用して、証明書のプロパティを検査し、関連する秘密キーがどこに保存されているかを判断できます。

承認証明書の検査

FAS管理コンソールで**authorization certificate**リンクをクリックすると、承認証明書を表示できます。

承認証明書(/en-us/federated-authentication-service/2511/media/auth-cert-config.png)

ただし、より詳細な情報についてはPowerShellを使用してください。

```
Get-FasAuthorizationCertificate -Address localhost -FullCertInfo
```

いくつかのフィールドが返されます。その中には、証明書が作成および保存されたプロバイダーを示す**PrivateKeyProvider**が含まれます。

PRIVATEKEYPROVIDER	キーの保存場所
マイクロソフト ソフトウェア キー ストレージ プロバイダー	キーはディスクに保存され、Microsoftのソフトウェアプロバイダーによって保護されています。
マイクロソフト プラットフォーム 暗号化プロ バイダー	キーはTPM（物理または仮想）に保存されます。
HSMベンダーキーストレージプロバイダー （例のみ）	キーはHSMに保存されます（この例では、ベンダーのプロバイダーは HSM Vendor Key Storage Provider という名前です）。

ユーザー証明書の検査

FASサーバーにキャッシュされているすべてのユーザー証明書のリストを次のように取得できます。

```
Get-FasUserCertificate -Address localhost -KeyInfo $true
```

KeyInfo パラメーターを使用すると、出力に証明書に関連付けられた秘密キーに関する詳細情報が含まれます。特に、**PrivateKeyProvider** フィールドは、証明書に関連付けられたキーペアがどこに保存されているかを示します（この値の解釈については、前のセクションを参照してください）。

`-UserPrincipalName` のようなさまざまなオプションパラメーターを使用して、返される証明書のセットをフィルターできます。

コマンド出力の証明書フィールドは、PEMエンコードされたユーザー証明書です。Windows証明書GUIを使用して証明書を表示するには、テキストを `.crt` ファイルにコピーします。

コマンド	説明
<pre>\$CertInfos = Get-FasUserCertificate -Address localhost</pre>	このリストには複数のユーザー証明書が含まれている場合があります。
<pre>\$CertInfo = \$CertInfos[0]</pre>	この例では、最初のユーザー証明書を選択します。
<pre>\$CertInfo.Certificate > c: \temp\user.crt</pre>	PEMデータを <code>.crt</code> ファイルにパイプします。
<pre>c:\temp\user.crt</pre>	Windows GUIで <code>.crt</code> ファイルを開きます。

Citrix Virtual Apps and Desktops 2411より前のFASバージョンからのアップグレード

Citrix Virtual Apps and Desktops 2411より前のFASリリースでは、秘密キーのプロパティは、次の場所にあるXMLファイルを編集して構成されていました。

```
%programfiles%\Citrix\Federated Authentication  
Service\Citrix.Authentication.FederatedAuthenticationService.exe.config
```

これは、このドキュメントで説明されているPowerShellコマンドに置き換えられました。これらのコマンドは、より柔軟性があり、FASサーバーを再起動せずに適用できます。

さらに、XMLファイルの設定とは異なり、PowerShellを使用して行われた構成は、FASサーバーがアップグレードされても保持されます。

秘密キーの構成に関連するXMLファイルの設定は、対応するPowerShellパラメーター（`Get-FasKeyConfig` および `Set-FasKeyConfig` で使用されているもの）とともに、次のようにリストされています。

XMLファイル設定	XMLファイルのデフォルト値	POWERSHELLの同等物	コメント
<code>Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.KeyLength</code>	2048	-長さ	-
<code>Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.KeyProtection</code>	GenerateNonExportableKey	<code>-Exportable</code> <code>-UseDefaultTpmProvider</code>	• <code>-Exportable</code> を <code>\$true</code> に設定することで、NoProtection が実現されます <code>-Exportable</code> を <code>\$false</code> に設定することで、<code>-GenerateNonExportableKey</code> が実現されます <code>-UseDefaultTpmProvider</code>

XMLファイル設定	XMLファイルのデフォルト値	POWERSHELLの同等物	コメント
			<code>vider</code> スイッチを指定することで、 <code>-GenerateTPMProtectedKey</code> が実現されます
<code>Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.ProviderLegacyCsp</code>	偽	-Ksp	<code>-Ksp</code> を <code>\$true</code> に設定することで、 <code>-ProviderLegacyCsp false</code> が実現されます <code>-ProviderLegacyCsp true</code> は、 <code>-Ksp</code> を <code>\$false</code> に設定することで実現されます
<code>Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.ProviderName</code>	-	-プロバイダー	-
<code>Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.ProviderType</code>	-	-CspType	-

XML構成のデフォルトとPowerShellのデフォルトは機能的に同等です。つまり、デフォルトでは、このバージョンおよびCitrix Virtual Apps and Desktops 2411より前のバージョンでFASによって生成されたキーペアのプロパティは同じです。

したがって、XML構成ファイルで上記のいずれの設定も変更していない場合は、FASをアップグレードする際に何もアクションを実行する必要はありません。

ただし、上記のいずれかの設定を変更した場合は、次のようにFASをアップグレードしてください。

- FASをメンテナンスモードにします。[メンテナンスモード](#)。
- FASインストーラーを実行するだけでFASをインプレースアップグレードします。アップグレード後、以前の設定はすべてXMLファイルに存在なくなり、XMLファイルで構成することはできません。
- [キー構成PowerShellコマンド](#) で説明されているように、PowerShellコマンド `Set-FasKeyConfig` を使用して、FAS秘密キー構成を希望どおりに設定します。認証およびユーザー証明書に必要な設定を考慮してください。
- [秘密キー構成のテスト](#) で説明されているように、構成をテストします
- FASサーバーをメンテナンスモードから解除します

次回アップグレードする際、FAS秘密キー構成設定は保持され、特別な操作を行う必要はありません。

暗号化リモート処理

FASユーザー証明書に関連付けられた秘密キーは、VDAに転送されることはありません。代わりに、VDAがユーザーのFAS証明書をVDAへのサインインまたはセッション内使用のために使用する必要がある場合、暗号化要求はFASサーバーにリモート処理されます。これにより、秘密キーがFASキー記憶域（ソフトウェア記憶域、TPM、またはHSMのいずれであっても）から離れることがないため、セキュリティが向上します。

Windows VDAでは、これはVDA上のプロバイダーのペアを使用することで実現されます。暗号化要求を行うアプリケーションまたはオペレーティングシステムコードは、操作がFASサーバーにリモート処理されていることを認識しません。

Citrix Virtual Apps and Desktops 2411より前は、プロバイダーは暗号化サービスプロバイダー (CSP) でした。アプリケーションおよびオペレーティングシステムコードのアクセスは、古いWindows CAPI APIを介して行われました。プロバイダーは次のとおりです。

- `CitrixLogonCsp.dll` : VDAへのシングルサインオン用

- `CitrixVirtualSmartcardCsp.dll` : セッション内証明書用

Citrix Virtual Apps and Desktops 2411以降、追加のキー記憶域プロバイダー (KSP) がVDAに提供されます。アプリケーションおよびオペレーティングシステムコードは、新しいWindows CNG APIを使用してこれらにアクセスします。新しいプロバイダーは次のとおりです。

- `CitrixLogonKsp.dll` : VDAへのシングルサインオン用
- `CitrixVirtualSmartcardKsp.dll` : セッション内証明書用

KSPは、Windowsアプリケーションに暗号化操作を公開する、より最新の方法であり、より多くの機能を提供します。例:

- ECCキーを持つ証明書がサポートされています
- 確率的署名方式 (PSS) パディングがサポートされています

FASとVDAの両方がCitrix Virtual Apps and Desktops 2411以降を実行している場合、KSPリモート処理（つまり、新しいKSPを介したリモート処理）が使用されます。それ以外の場合、システムは古いCSPを使用してリモート処理にフォールバックします。

KSPリモート処理の無効化

互換性の問題が発生した場合、KSPリモート処理を無効にして、常に古いCSPリモート処理を使用できるようにすることが可能です。

次のPowerShellを使用します。

```
Set-FasServer -Address localhost -KspRemoting $false
```

メンテナンスモード

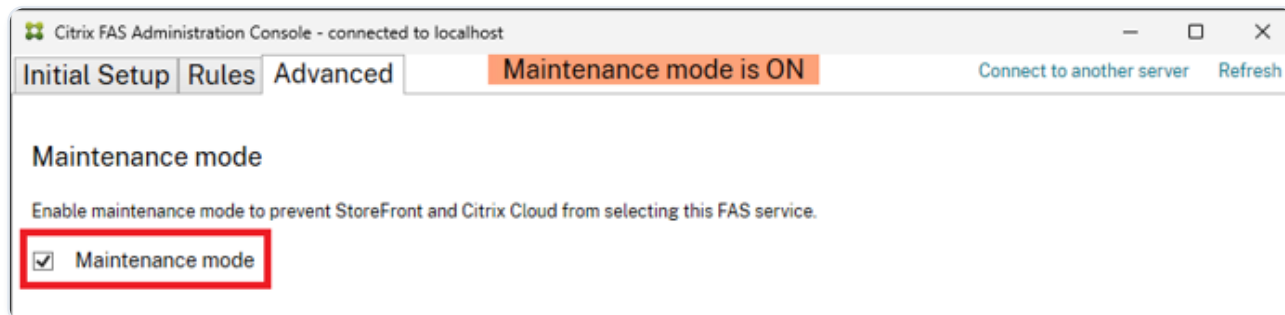
稼働中のFASサーバーの構成に変更を加える際は、メンテナンスモードにすることを検討してください。

FASがメンテナンスモードの場合、以下が適用されます。

- **Workspace**または**StoreFront™**が公開アプリケーションまたはデスクトップの起動シーケンスの一部としてFASを呼び出す際、FASはメンテナンスモードであることを示します。呼び出し元は、別のFASサーバーを選択することでこれに対応する必要があります。
- 追加の予防措置として、FASはメンテナンスモード中にユーザー証明書の自動作成を許可しません。これにより、意図しない設定でのユーザー証明書の誤った作成が回避されます。
- ただし、VDAサインインやセッション内使用など、既存のユーザー証明書に関連するアクティビティは引き続き許可されます。

ユーザー証明書の自動作成は許可されていませんが、管理者は `New-FasUserCertificate` や `Test-FasCertificateSigningRequest` などのPowerShellコマンドを使用してユーザー証明書を作成できます。

管理コンソールの使用



PowerShellの使用

FASサーバーをメンテナンスモードにするには、次のようにします。

```
Set-FasServer -Address localhost -MaintenanceMode $true
```

FASサーバーをメンテナンスモードから解除し（通常の操作に戻し）、次のようにします。

```
Set-FasServer -Address localhost -MaintenanceMode $false
```

関連情報

- [インストールと構成](#) は、FASのインストールと構成に関する主要なリファレンスです。
- 一般的なFAS展開は、[フェデレーション認証サービスアーキテクチャの概要](#) 記事にまとめられています。
- その他のハウツー記事は、[高度な構成](#) 記事で紹介されています。

セキュリティとネットワーク構成

Federated Authentication Service (FAS) は、Microsoft Active Directory および Microsoft 証明機関と密接に統合されています。ドメインコントローラーやその他の重要なインフラストラクチャと同様に、システムが適切に管理および保護されるようにし、セキュリティポリシーを策定してください。

このドキュメントでは、FAS を展開する際に考慮すべきセキュリティ問題の概要を説明します。また、インフラストラクチャの保護に役立つ可能性のある利用可能な機能の概要も提供します。

ネットワークアーキテクチャとセキュリティ

次の図は、FAS 展開で使用される主要なコンポーネントとセキュリティ境界を示しています。

FAS サーバーは、証明機関およびドメインコントローラーとともに、セキュリティ上重要なインフラストラクチャの一部です。フェデレーション環境では、Citrix Gateway と Citrix StoreFront はユーザー認証を実行するコンポーネントです。その他の Citrix Virtual Apps and Desktops™ コンポーネントは、FAS の導入による影響を受けません。

サーバーとプロトコルを示す図 (/en-us/federated-authentication-service/2511/media/fas-security-network.png)

サーバー	接続
フェデレーション認証サービス	[in] StoreFront™ および VDA からの Kerberos セキュリティによる HTTP、[out] Microsoft 証明機関への DCOM
シトリックス ゲートウェイ	[in] クライアントマシンからの HTTPS、[in/out] StoreFront サーバーへの/からの HTTPS、[out] VDA への HDX
StoreFront	[in] Citrix Gateway からの HTTPS、[out] Delivery Controller™ への HTTPS、[out] FAS への Kerberos セキュリティによる HTTP
デリバリーコントローラー	StoreFrontサーバーからの[in] HTTPS、VDAからのKerberosセキュリティによる[in/out] HTTP
VDA	デリバリーコントローラーからのKerberosセキュリティによる[in/out] HTTP、Citrix Gatewayからの[in] HDX、FASへのKerberosセキュリティによる[out] HTTP
Microsoft証明機関	FASからの[in] DCOM

StoreFrontとFAS間の通信

- VDAを起動すると、StoreFrontサーバーはFASサーバーに接続し、Citrix Virtual Delivery Agent (VDA) がユーザーをサインインさせるために必要な使い捨てチケットを取得します。
- StoreFrontは、SOAP over HTTPを使用してFASに接続します。デフォルトではポート80を使用します。

- FASサーバーのKerberos HOST/fqdn IDとStoreFrontサーバーのKerberosマシンアカウントIDを使用して、相互Kerberos認証を行います。
- データはメッセージレベルセキュリティを使用して暗号化されます。暗号化を有効にするための追加設定は不要です。

VDAとFAS間の通信

HDX™セッションがVDAに接続されると、VDAはFASサーバーに接続して証明書を要求します。

- VDAは、SOAP over HTTPを使用してFASサーバーに接続します。デフォルトではポート80を使用します。
- FASサーバーのKerberos HOST/fqdn IDとVDAのKerberosマシンIDを使用して、相互Kerberos認証を行います。また、VDAは証明書と秘密鍵にアクセスするために「credential handle」を提供する必要があります。
- データはメッセージレベルセキュリティを使用して暗号化されます。暗号化を有効にするための追加設定は不要です。

FASとMicrosoft証明機関間の通信

ユーザーがVDAを起動したときに、FASサーバーがそのユーザーの証明書をまだ持っていない場合、証明書を要求するために証明機関と通信します。証明機関は、信頼された登録エージェント証明書によって署名されたCMCパケットをFASサーバーが提供することを要求します。

- FASサーバーはDCOMを使用してMicrosoft証明機関と通信します。必要なポートについては、[Microsoftドキュメント](#)を参照してください。
- Kerberosを使用して認証します。

シトリックス フェデレーテッド認証サービスとCitrix Cloud™間の接続

FASをCitrix Cloudに接続する場合、FASサーバーはHTTPSポート443経由で次のアドレスにアクセスする必要があります。

シトリックス クラウド：

- ユーザーアカウントで実行されるFAS管理コンソール
 - *.cloud.com
 - *.citrixworkspacesapi.net
 - 環境でサードパーティのIDプロバイダーを使用している場合に、そのプロバイダーが必要とするアドレス

- Network Serviceアカウントで実行されるFASサービス:

- *.citrixworkspacesapi.net
- *.citrixnetworkapi.net

シトリックス クラウド ジャパン:

- ユーザーアカウント下のFAS管理コンソール

- *.citrixcloud.jp
- *.citrixworkspacesapi.jp
- 環境でサードパーティのIDプロバイダーを使用している場合、そのプロバイダーが必要とするアドレス

- ネットワークサービスアカウント下のFASサービス:

- *.citrixworkspacesapi.jp
- *.citrixnetworkapi.jp

環境にプロキシサーバーが含まれている場合は、FAS管理コンソールのアドレスを使用してユーザープロキシを構成します。また、netshまたは同様のツールを使用して、ネットワークサービスアカウントのアドレスが構成されていることを確認してください。

詳細情報

他のCitrixコンポーネント間の通信を保護する方法については、以下の記事を参照してください。

- [Citrix Virtual Apps and Desktops - セキュリティに関する考慮事項とベストプラクティス。](#)
- [StoreFront展開の保護。](#)

セキュリティに関する考慮事項

FASには、ドメインユーザー向けに自律的に証明書を発行できる登録機関証明書があります。これにより、FASサーバーを保護し、その権限を制限するためのセキュリティポリシーの開発と実装に役立ちます。

委任された登録エージェント

FAS は登録エージェントとして機能することで、ユーザー証明書を発行します。Microsoft 証明機関では、登録エージェント、証明書テンプレート、および登録エージェントが証明書を発行できるユーザーを制限できます。

登録エージェントダイアログ(/en-us/federated-authentication-service/2511/media/delegated-enrollment-agents.png)

このダイアログを使用して、以下を確認できます。

- 「登録エージェント」リストには、FAS サーバーのみが含まれていること（Active Directory 展開で他の登録エージェントが不要であると仮定した場合）。
- 「証明書テンプレート」リストには、ユーザー証明書の発行に使用される FAS テンプレートのみが含まれていること。デフォルトでは、これは Citrix_SmartcardLogon テンプレートです。
- 「アクセス許可」リストには、FAS の使用が許可されているユーザーが含まれていること。たとえば、管理者または保護されたユーザーグループに証明書を発行しないことをお勧めします。

注：

コンピューターアカウントの Active Directory グループメンバーシップへの変更は、コンピューターが再起動されるまで有効になりません。

アクセス制御リストの構成

ルールを構成するセクションで説明されているように、StoreFront サーバーのリストを構成する必要があります。これらの StoreFront サーバーは、証明書が発行されるときに FAS にユーザー ID をアサートします。同様に、証明書が発行されるユーザーと、認証できる VDA マシンを制限できます。この機能は、構成する標準の Active Directory または証明機関のセキュリティ機能に追加されるものです。

ファイアウォール設定

FAS サーバーは、別途構成されていない限り、ポート 80 を使用して StoreFront および VDA からの受信接続を受け入れる必要があります。ネットワーク通信の詳細については、ネットワークアーキテクチャとセキュリティを参照してください。

FAS インストーラーは、オプションで Windows ファイアウォールを構成できます。詳細については、FAS インストーラーオプションを参照してください。

FAS サーバーポートの変更

FASサーバーはデフォルトでポート80を使用します。ポートはカスタマイズできます。

注：

FASサーバーのポートをポート443に変更できますが、FASが使用するプロトコルは変更されません。FASはポート443で構成されていてもHTTPSを使用しません。

1. FASサーバーで次のコマンドラインを実行します。

```
"C:\Program Files\Citrix\Federated Authentication  
Service\Citrix.Authentication.FederatedAuthenticationService.exe" /  
SVCPORT [port] /CONFIGUREFIREWALL
```

[port] を使用したいポート番号に置き換えます。

/CONFIGUREFIREWALL スイッチにより、Windowsファイアウォールが更新され、指定されたポートでの受信接続が許可されます。

2. FASサービスを再起動します。
3. FASグループポリシーオブジェクトで、FASサーバーのリストを更新してポートを含めます（例： `fas.example.com:[port]` ）。
4. 変更をFASサーバー、StoreFront、およびVDAに伝播します（例： `gpupdate /force` を使用）。

イベントログの監視

FASとVDAはWindowsイベントログに情報を書き込みます。このログは、監視および監査情報に使用できます。[イベントログ](#) セクションには、生成される可能性のあるイベントログエントリが一覧表示されます。

ハードウェアセキュリティモジュール

FASによって発行されたユーザー証明書キーを含むすべての秘密キーは、ネットワークサービスアカウントによってエクスポート不可能な秘密キーとして保存されます。セキュリティポリシーで必要とされる場合、FASは暗号化ハードウェアセキュリティモジュール（HSM）の使用をサポートします。

低レベルの暗号化構成は、**PowerShell** コマンドを使用して利用できます。FAS認証証明書の秘密キーとユーザー証明書キーには、異なる設定を使用できます。詳細については、「[秘密キーの保護](#)」を参照してください。

管理者の責任

環境の管理は、以下のグループに分けられます。

名前	責任
エンタープライズ管理者	フォレスト内の証明書テンプレートをインストールして保護する
ドメイン管理者	グループポリシー設定を構成する
証明機関管理者	証明機関を構成する
FAS管理者	FASサーバーをインストールして構成する
StoreFront/Citrix Gateway管理者	ユーザー認証を構成する
シトリックス バーチャル デスクトップス™ 管理者	VDAとコントローラーを構成する

各管理者は、全体的なセキュリティモデルの異なる側面を制御し、システムを保護するための多層防御アプローチを可能にします。

グループポリシー設定

注：

すべてのFASサーバーとVDAがバージョン2511以降の場合、VDA上のグループポリシーFQDNリストは不要になります。(/ja-jp/federated-authentication-service/2511/config-manage/fas-v2-ticketing-and-registry-address-list.html)「FAS V2チケットティングとレジストリアドレスリスト」を参照してください。

信頼されたFASマシンは、グループポリシーを通じて構成された「インデックス番号 -> FQDN」のルックアップテーブルによって識別されます。FASサーバーに接続する際、クライアントはFASサーバーの `HOST\<fqdn>` Kerberos IDを検証します。FASサーバーにアクセスするすべてのサーバーは、同じインデックスに対して同一のFQDN構成を持つ必要があります。そうでない場合、StoreFrontとVDAは異なるFASサーバーに接続する可能性があります。さらに、FASサーバーがCitrix Cloudに接続されている場合、グループポリシーはFASサーバー自体にも適用される必要があります。

Citrixは、誤った構成を避けるために、環境内のすべてのマシンに単一のポリシーを適用することを推奨します。FASサーバーのリストを変更する際には、特にエントリの削除や並べ替えを行う際には注意してください。

このGPOの制御は、FASサーバーをインストールおよび廃止するFAS管理者（および/またはドメイン管理者）に限定する必要があります。FASサーバーを廃止した直後にマシンのFQDN名を再利用しないように注意してください。

FASグループポリシー設定は、レジストリの

`HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\Authentication` に表示されます。グループポリシーからのFAS FQDNのリストは、サブキー

`HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\Authentication\UserCredentialService\Addresses` に表示されます。

証明書テンプレート

FASに付属のCitrix_SmartcardLogon証明書テンプレートを使用しない場合は、そのコピーを変更できます。以下の変更がサポートされています。

証明書テンプレートの名前を変更する

Citrix_SmartcardLogonの名前を組織のテンプレート命名標準に合わせたい場合は、次の操作を行う必要があります。

- 証明書テンプレートのコピーを作成し、組織のテンプレート命名標準に合うように名前を変更します。
- 管理者ユーザーインターフェイスではなく、FAS PowerShellコマンドを使用してFASを管理します。（管理者ユーザーインターフェイスは、Citrixのデフォルトテンプレート名でのみ使用することを目的としています。）
 - Microsoft MMC証明書テンプレートスナップインまたはPublish-FasMsTemplateコマンドのいずれかを使用してテンプレートを公開します。
 - New-FasCertificateDefinitionコマンドを使用して、テンプレート名でFASを構成します。

一般プロパティの変更

デフォルトでは、ユーザー証明書の有効期間は7日間です。証明書テンプレートで有効期間を変更できます。

更新期間は変更しないでください。FASは証明書テンプレートのこの設定を無視します。FASは、証明書の有効期間の途中で自動的に証明書を更新します。

要求処理プロパティの変更

これらのプロパティは変更しないでください。FASは証明書テンプレートのこれらの設定を無視します。

FASが提供する設定については、[秘密キーの保護](#)を参照してください。

暗号化プロパティの変更

これらのプロパティは変更しないでください。FASは証明書テンプレートのこれらの設定を無視します。

FASが提供する同等の設定については、[秘密キーの保護](#)を参照してください。

キー証明プロパティの変更

これらのプロパティは変更しないでください。FASはキー証明をサポートしていません。

廃止されたテンプレートプロパティの変更

これらのプロパティは変更しないでください。FASはテンプレートの廃止をサポートしていません。

拡張プロパティの変更

これらの設定を組織のポリシーに合わせて変更できます。

注：

不適切な拡張設定は、セキュリティ上の問題を引き起こしたり、使用できない証明書になったりする可能性があります。

セキュリティプロパティの変更

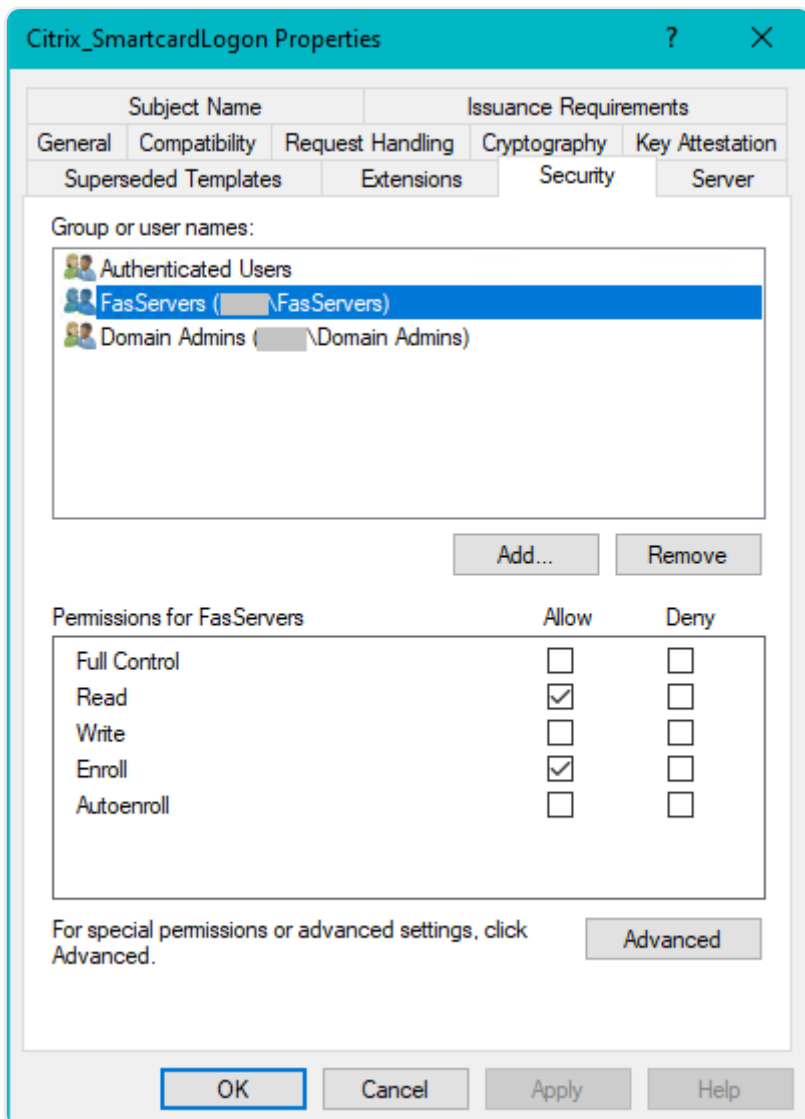
Citrixでは、これらの設定を変更して、FASサーバーのコンピューターアカウントのみに**読み取り**および**登録**のアクセス許可を付与することをお勧めします。FASサービスは、その他のアクセス許可を必要としません。

さらに：

- **認証済みユーザー**がテンプレートを**読み取る**ことを許可します。これは、証明機関自体がテンプレートを**読み取る**必要があるため、必須です。
- 証明機関の管理者がテンプレートを**読み取り**および**書き込む**ことを許可します。

この推奨事項は、3つのFASテンプレートすべてに適用されます。

- Citrix_SmartcardLogon
- Citrix_RegistrationAuthority
- Citrix_RegistrationAuthority_ManualAuthorization



注：

コンピューターアカウントのActive Directoryグループメンバーシップに対する変更は、コンピューターが再起動されるまで有効になりません。

サブジェクト名のプロパティを変更する

Citrixでは、これらのプロパティを変更しないことをお勧めします。

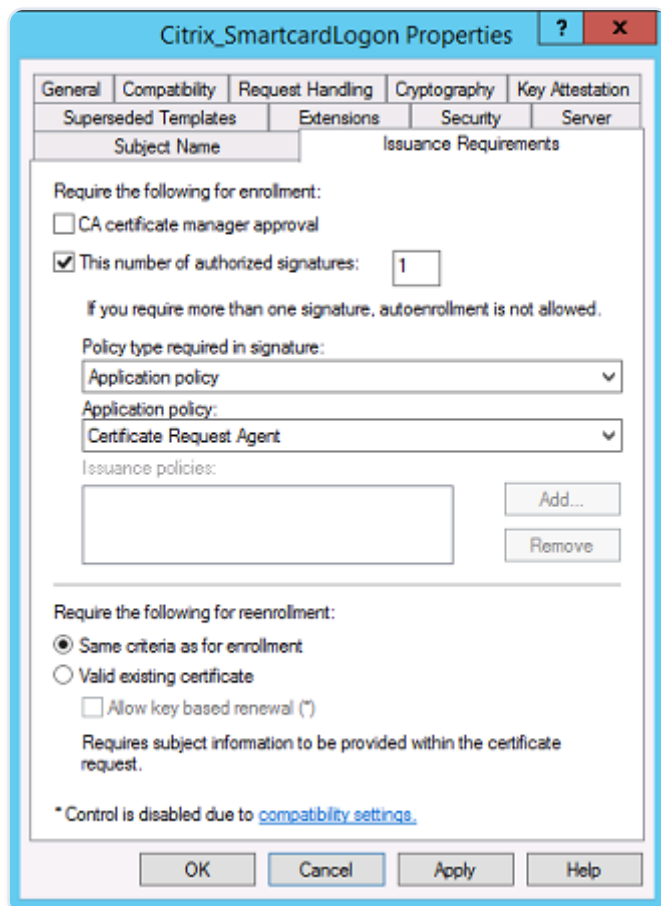
テンプレートで が選択されているため、証明機関はユーザーのSIDを証明書拡張機能に含め、ユーザーのActive Directoryアカウントへの強力なマッピングを提供します。

サーバーのプロパティを変更する

Citrixでは推奨していませんが、必要に応じて、組織のポリシーに合わせてこれらの設定を変更できます。

発行要件のプロパティを変更する

これらの設定は変更しないでください。これらの設定は次のようにする必要があります。



互換性のプロパティを変更する

これらの設定は変更できます。設定は少なくとも **Windows Server 2003 CA**（スキーマバージョン2）である必要があります。ただし、FASはWindows Server 2008以降のCAのみをサポートします。また、前述のとおり、FASは **Windows Server 2008 CA**（スキーマバージョン3）または **Windows Server 2012 CA**（スキーマバージョン4）を選択することで利用できる追加設定を無視します。

証明機関の管理

証明機関管理者は、証明機関サーバーの構成と、それが使用する発行証明書の秘密キーに責任を負います。

テンプレートの公開

証明機関がエンタープライズ管理者によって提供されたテンプレートに基づいて証明書を発行するには、証明機関管理者がそのテンプレートを公開することを選択する必要があります。

簡単なセキュリティ対策として、FASサーバーのインストール時に登録機関の証明書テンプレートのみを公開するか、完全にオフラインの発行プロセスを要求する方法があります。いずれの場合も、証明機関管理者は登録機関の証明書要求の承認を完全に制御し、FASサーバーを承認するためのポリシーを維持する必要があります。

ファイアウォール設定

証明機関管理者は、証明機関のネットワークファイアウォール設定を制御し、受信接続を制御できます。証明機関管理者は、FASサーバーのみが証明書を要求できるように、DCOM TCPおよびファイアウォールルールを構成できます。

登録の制限

デフォルトでは、登録機関証明書の所有者は、アクセスを許可する任意の証明書テンプレートを使用して、任意のユーザーに証明書を発行できます。Citrixでは、**登録エージェントの制限**証明機関プロパティを使用して、証明書の発行を非特権ユーザーのグループに制限することを推奨しています。[委任された登録エージェント](#)を参照してください。

ポリシーモジュールと監査

高度な展開では、カスタムセキュリティモジュールを使用して、証明書の発行を追跡および拒否できます。

FAS管理

FASにはいくつかのセキュリティ機能があります。

ACLによるStoreFront、ユーザー、およびVDAの制限

FASセキュリティモデルの中心は、どのKerberosアカウントが機能にアクセスできるかを制御することです。

アクセスベクター	説明
StoreFront [IdP]	これらのKerberosアカウントは、ユーザーが正しく認証されたことを宣言するために信頼されています。これらのアカウントのいずれかが侵害された場合、FASの構成によって許可さ

アクセスベクター	説明
	れたユーザーに対して証明書が作成され、使用される可能性があります。
VDA [Relying party]	これらは、証明書と秘密キーへのアクセスが許可されているマシンです。IdPによって取得された資格情報ハンドルも必要であるため、このグループ内の侵害されたVDAアカウントがシステムを攻撃できる範囲は限られています。
ユーザー	このオプションは、どのユーザーがIdPによってアサートされるかを制御します。証明機関の「制限付き登録エージェント」構成オプションと重複する点があることに注意してください。一般に、このリストには非特権アカウントのみを含めることをお勧めします。これにより、侵害されたStoreFrontアカウントがより高い管理レベルに特権を昇格させるのを防ぎます。特に、ドメイン管理者アカウントはこのACLによって許可されてはなりません。

ルールの構成

複数の独立したCitrix Virtual Apps™またはCitrix Virtual Desktops展開が同じFASサーバーインフラストラクチャを使用する場合、ルールは役立ちます。各ルールには個別の構成オプションセットがあり、特にKerberosアクセス制御リスト（ACL）は個別に構成できます。

証明機関とテンプレートの構成

異なるアクセス権に対して、異なる証明書テンプレートとCAを構成できます。高度な構成では、環境に応じて、より強力な証明書またはより強力でない証明書を使用することを選択できます。たとえば、「外部」として識別されたユーザーは、「内部」ユーザーよりも少ない特権を持つ証明書を持つことができます。

セッション内証明書と認証証明書

FAS管理者は、認証に使用される証明書がユーザーセッション内で使用可能であるかどうかを制御できます。たとえば、ユーザーはセッション内で「署名」証明書のみを使用でき、より強力な「ログオン」証明書はログオン時にのみ使用できます。

秘密キーの保護とキーの長さ

FAS管理者は、秘密キーをハードウェアセキュリティモジュール（HSM）またはトラステッドプラットフォームモジュール（TPM）に保存するようにFASを構成できます。Citrixは、少なくともFAS認証証明書の秘密キーをTPMに保存して保護することを推奨しています。

同様に、ユーザー証明書の秘密キーはTPMまたはHSMに保存できます。すべてのキーはエクスポート不可として生成され、RSAを使用する場合は少なくとも2048ビットの長さである必要があります。

注：

FASはユーザー証明書キーをTPMまたはHSMで生成および保存できますが、大規模な展開ではハードウェアが遅すぎたり、サイズが制約されたりする場合があります。

詳細については、「[秘密キーの保護](#)」を参照してください。

イベントログ

FASサーバーは、詳細な構成とランタイムのイベントログ([/ja-jp/federated-authentication-service/2511/config-manage/troubleshoot-logon.html#fas-event-logs](#))を提供し、監査および侵入検知に使用できます。

管理アクセスと管理ツール

FASには、リモート管理機能（相互認証Kerberos）とツールが含まれています。「ローカル管理者グループ」のメンバーは、FAS構成を完全に制御できます。FAS構成は適切に維持する必要があります。

シトリックス バーチャル アプリケーションズ、シトリックス バーチャル デスクトップ、およびVDA管理者

FASの使用は、Delivery ControllerおよびVDA管理者のセキュリティモデルを変更しません。FASの「資格情報ハンドル」は単に「Active Directoryパスワード」を置き換えるだけだからです。ControllerおよびVDA管理グループには、信頼できるユーザーのみを含める必要があります。監査およびイベントログは維持する必要があります。

一般的なWindowsサーバーのセキュリティ

すべてのサーバーは完全にパッチが適用され、標準のファイアウォールおよびウイルス対策ソフトウェアが利用可能である必要があります。セキュリティ上重要なインフラストラクチャサーバー

は、物理的に安全な場所に保管し、ディスク暗号化と仮想マシンのメンテナンスオプションに注意を払う必要があります。

監査およびイベントログは、リモートマシンに安全に保存する必要があります。

RDPアクセスは、許可された管理者に限定する必要があります。Citrixは、ユーザーアカウント、特に証明機関およびドメイン管理者アカウントに対してスマートカードログオンを推奨しています。

連邦情報処理標準（FIPS）のサポート

FASは、FIPS対応Windowsコンピューターで[FIPS検証済み暗号化アルゴリズム](#)を使用します。キーの保存にTPMまたはHSMを使用するようにFASを構成する場合は、FIPS準拠情報についてハードウェアベンダーにお問い合わせください。

関連情報

- インストールと構成(</ja-jp/federated-authentication-service/2511/install-configure.html>)は、FASのインストールと構成に関する主要なリファレンスです。
- FASアーキテクチャは、展開アーキテクチャ(</ja-jp/federated-authentication-service/2511/deployment-architectures.html>)の記事で紹介されています。
- その他の「ハウツー」記事は、[高度な構成](#)の記事で紹介されています。

パフォーマンスカウンター

FAS には、負荷追跡目的のパフォーマンスカウンターセットが含まれています。

ローカライズされた画像(</en-us/federated-authentication-service/2511/media/performance-counters.png>)

次の表に、利用可能なカウンターを示します。特に明記されていない限り、各カウンターは10秒ごとに更新されます。

名前	説明
平均証明書署名要求ミリ秒	直前の1分間のデータを使用して計算された、証明書署名要求の平均期間（ミリ秒単位）。
証明書数	Federated Authentication Service によって管理されている証明書の数。

名前	説明
1分あたりの証明書署名要求数	直前の1分間のデータを使用して計算された、Federated Authentication Service によって1分あたりに発行された証明書署名要求の数。
同時証明書署名要求数	Federated Authentication Service によって処理されている同時証明書署名要求の数。
プールキー数	証明書署名要求に使用できる、キープール内の事前生成されたキーペアの数。
1分あたりの秘密キー操作	フェデレーション認証サービスによって1分あたりに実行される証明書秘密キー操作の数。これは前の1分間のデータを使用して計算されます。
セッション数	フェデレーション認証サービスによって追跡されているVDAセッションの数。
低/中/高負荷レベル	フェデレーション認証サービスが1分あたりに受け入れられる証明書署名要求の観点からの負荷の見積もり。見積もりは、前の1分間のデータを使用して毎分更新されます。「高負荷」しきい値を超えると、公開されたアプリまたはデスクトップの起動が失敗する可能性があります。

Windowsログオンの問題のトラブルシューティング

この記事では、ユーザーが証明書またはスマートカード、あるいはその両方を使用してログオンする際にWindowsが提供するログとエラーメッセージについて説明します。これらのログは、認証の失敗をトラブルシューティングするために使用できる情報を提供します。

証明書と公開鍵インフラストラクチャ

Windows Active Directoryは、ログオンするユーザーの証明書を管理する複数の証明書ストアを保持しています。

- **NTAuth証明書ストア:** Windowsに認証するには、ユーザー証明書を直接発行する証明機関（つまり、チェーンはサポートされていません）をNTAuthストアに配置する必要があります。これ

らの証明書を表示するには、certutilプログラムから次のように入力します: `certutil -viewstore -enterprise NTAAuth`

- **ルートおよび中間証明書ストア:** 通常、証明書ログオンシステムは単一の証明書しか提供できないため、チェーンが使用されている場合、すべての中間証明書ストアにはこれらの証明書が含まれている必要があります。ルート証明書は信頼されたルートストアに、最後から2番目の証明書はNTAuthストアにある必要があります。
- **ログオン証明書拡張機能とグループポリシー:** Windowsは、EKUおよびその他の証明書ポリシーの検証を強制するように構成できます。Microsoftのドキュメントを参照してください: [https://docs.microsoft.com/ja-jp/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/ff404287\(v=ws.10\)>](https://docs.microsoft.com/ja-jp/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/ff404287(v=ws.10)>)。

レジストリポリシー	説明
AllowCertificatesWithNoEKU	無効にすると、証明書にはスマートカードログオンの拡張鍵使用法 (EKU) が含まれている必要があります。
AllowSignatureOnlyKeys	デフォルトでは、WindowsはRSA復号化を許可しない証明書の秘密鍵を除外します。このオプションはそのフィルターを上書きします。
AllowTimeInvalidCertificates	デフォルトでは、Windowsは期限切れの証明書を除外します。このオプションはそのフィルターを上書きします。
EnumerateECCerts	楕円曲線認証を有効にします。
X509ヒントが必要	証明書に一意のユーザープリンシパル名 (UPN) が含まれていない場合、またはそれが曖昧な場合、このオプションを使用すると、ユーザーはWindowsログオンアカウントを手動で指定できます。
UseCachedCRLOnlyAnd, IgnoreRevocationUnknownErrors	失効チェックを無効にします (ドメインコントローラーで設定)。

- **ドメインコントローラー証明書:** Kerberos接続を認証するには、すべてのサーバーに適切な「ドメインコントローラー」証明書が必要です。これらは、「ローカルコンピューター証明書個人ストア」MMCスナップインメニューを使用して要求できます。

UPN名と証明書のマッピング

ユーザー証明書には、サブジェクト代替名拡張に一意のユーザープリンシパル名 (UPN) を含めることをお勧めします。

Active DirectoryにおけるUPN名

デフォルトでは、Active Directoryのすべてのユーザーは、

`\<samUsername>@\<domainNetBios>` および `\<samUsername>@\<domainFQDN>` のパターンに基づいた暗黙的なUPNを持っています。利用可能なドメインとFQDNは、フォレストの **RootDSE** エントリに含まれています。単一のドメインは、RootDSEに複数のFQDNアドレスを登録できます。

また、Active Directoryのすべてのユーザーは、明示的なUPNと `altUserPrincipalNames` を持っています。これらは、ユーザーのUPNを指定するLDAPエントリです。

UPNでユーザーを検索する場合、Windowsはまず現在のドメイン（UPNを検索するプロセスのIDに基づく）で明示的なUPNを検索し、次に代替UPNを検索します。一致するものがない場合、暗黙的なUPNを検索します。これはフォレスト内の異なるドメインに解決される可能性があります。

証明書マッピングサービス

証明書に明示的なUPNが含まれていない場合、Active Directoryには、「x509certificate」属性に各使用の正確な公開証明書を保存するオプションがあります。このような証明書をユーザーに解決するために、コンピューターはこの属性を直接クエリできます（デフォルトでは、単一ドメイン内）。

ユーザーが検索を高速化するユーザーアカウントを指定するオプションが提供されており、この機能はクロスドメイン環境でも使用できます。

フォレスト内に複数のドメインがあり、ユーザーがドメインを明示的に指定しない場合、Active Directory の rootDSE が証明書マッピングサービスの場所を指定します。これはグローバルカタログマシンにあり、フォレスト内のすべての x509certificate 属性のキャッシュされたビューを持っています。このコンピューターは、証明書のみに基づいて、任意のドメイン内のユーザーアカウントを効率的に見つけるために使用できます。

ログオン ドメインコントローラーの選択を制御する

環境に複数のドメインコントローラーが含まれている場合、認証に使用されるドメインコントローラーを確認し、制限することは、ログを有効にして取得できるようにするために役立ちます。

ドメインコントローラーの選択を制御する

ログオン時に特定の Windows ドメインコントローラーを使用するように Windows を強制するには、lmhosts ファイル (\Windows\System32\drivers\etc\lmhosts) を構成することで、Windows マシンが使用するドメインコントローラーのリストを明示的に設定できます。

通常、その場所に「lmhosts.sam」という名前のサンプルファイルがあります。単に次の行を含めます。

```
1.2.3.4 dcnetbiosname #PRE #DOM:mydomai
```

ここで、「1.2.3.4」は **mydomain** ドメイン内の **dcnetbiosname** という名前のドメインコントローラーの IP アドレスです。

再起動後、Windows マシンはその情報を使用して **mydomain** にログオンします。この構成は、デバッグが完了したら元に戻す必要があります。

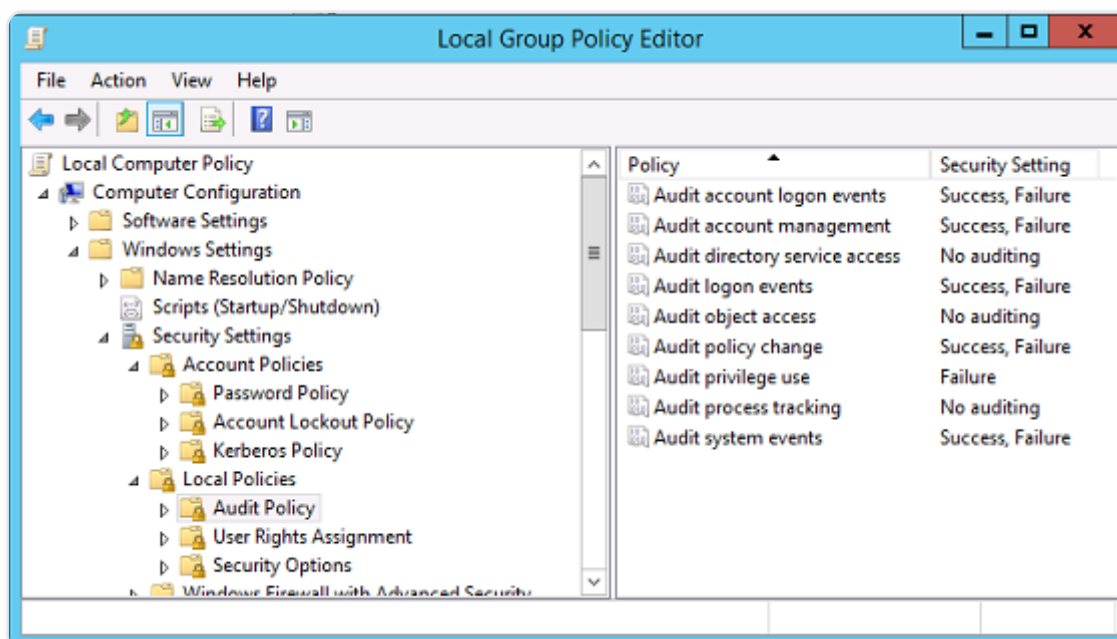
使用中のドメインコントローラーを特定する

ログオン時に、Windows はユーザーをログオンさせたドメインコントローラーを含む MSDOS 環境変数を設定します。これを確認するには、コマンドプロンプトを起動し、**echo %LOGONSERVER%** コマンドを実行します。

認証に関連するログは、このコマンドによって返されるコンピューターに保存されます。

アカウント監査イベントを有効にする

デフォルトでは、Windows ドメインコントローラーは完全なアカウント監査ログを有効にしていません。これは、グループポリシーエディターのセキュリティ設定にある監査ポリシーを通じて制御できます。グループポリシーエディターを開くには、ドメインコントローラーで **gpedit.msc** を実行します。監査ポリシーが有効になると、ドメインコントローラーはセキュリティログに追加のイベントログ情報を生成します。



証明書検証ログ

証明書の有効性を確認する

スマートカード証明書がDER証明書としてエクスポートされた場合（秘密鍵は不要）、次のコマンドで検証できます: `certutil -verify user.cer`

CAPIログを有効にする

ドメインコントローラーとユーザーのマシンで、イベントビューアーを開き、Microsoft/Windows/CAPI2/Operational Logs のログを有効にします。

ドメインコントローラーとVDAマシンで、イベントビューアーを開き、**アプリケーションとサービスログ > Microsoft > Windows > CAPI2 > Operational** に移動します。**Operational** を右クリックし、**ログの有効化** を選択します。

さらに、レジストリ値 `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\crypt32` で CAPI ログを微調整します。以下の値はデフォルトでは存在しません。これらを作成する必要があります。デフォルトのCAPI2ログ設定に戻したい場合は、これらの値を削除してください。

値	説明
DiagLevel (DWORD)	詳細レベル (0～5)
DiagMatchAnyMask (QUADWORD)	イベントフィルター (すべてに 0xffffffff を使用)
DiagProcessName (MULTI_SZ)	プロセス名でフィルタリング (例: LSASS.exe)

CAPIログ

メッセージ	説明
チェーンの構築	LSAがCertGetCertificateChainを呼び出し (結果を含む)
失効の検証	LSAがCertVerifyRevocationを呼び出し (結果を含む)
X509オブジェクト	詳細モードでは、証明書と証明書失効リスト (CRL) が AppData\LocalLow\Microsoft\X509Objectsにダンプされます
チェーンポリシーの検証	LSAがCertVerifyChainPolicyを呼び出し (パラメータを含む)

エラーメッセージ

エラーコード	説明
証明書が信頼されていません	スマートカード証明書を、コンピューターの中間証明書ストアおよび信頼されたルート証明書ストアにある証明書を使用して構築できませんでした。
証明書失効チェックエラー	スマートカードのCRLを、証明書のCRL配布ポイントで指定されたアドレスからダウンロードできませんでした。失効チェックが必須の場合、これによりログオンが成功しません。 (/ja-jp/federated-authentication-service/2511/config-manage/troubleshoot-logon.html#certificates-and-public-key-infrastructure)セクション「証明書と公開鍵インフラストラクチャ」を参照してください。
証明書使用エラー	この証明書はログオンに適していません。たとえば、サーバー証明書または署名証明書である可能性があります。

Kerberosログ

Kerberosログを有効にするには、ドメインコントローラーとエンドユーザーマシンで、次のレジストリ値を作成します。

ハイブ	値の名前	値 [DWORD]
CurrentControlSet\Control\LSA\Kerberos\Parameters	LogLevel	0x1
CurrentControlSet\Control\LSA\Kerberos\Parameters	KerbDebuglevel	0xffffffff
CurrentControlSet\Services\Kdc	KdcDebugLevel	0x1
CurrentControlSet\Services\Kdc	KdcExtraLogLevel	0x1f

Kerberosログはシステムイベントログに出力されます。

- 信頼されていない証明書のようなメッセージは、診断しやすい必要があります。
- 2つのエラーコードは情報提供であり、安全に無視できます。
 - KDC_ERR_PREAUTH_REQUIRED (古いドメインコントローラーとの下位互換性のために使用されます)
 - 不明なエラー 0x4b

ドメインコントローラーおよびワークステーションログ

このセクションでは、ユーザーが証明書でログオンしたときのドメインコントローラーとワークステーション上の予期されるログエントリについて説明します。

- ドメインコントローラー CAPI2 ログ
- ドメインコントローラー セキュリティログ
- Virtual Delivery Agent (VDA) セキュリティログ
- VDA CAPI ログ
- VDA システムログ

ドメインコントローラー CAPI2 ログ

ログオン中、ドメインコントローラーは呼び出し元の証明書を検証し、次の形式で一連のログエントリを生成します。

ドメインコントローラー CAPI2 ログ (/en-us/federated-authentication-service/2511/media/fas-troubleshoot-logon-capi2-log.png)

最終的なイベントログメッセージは、ドメインコントローラー上の lsass.exe が VDA から提供された証明書に基づいてチェーンを構築し、その有効性（失効を含む）を検証していることを示しています。結果は「ERROR_SUCCESS」として返されます。

ドメインコントローラー CAPI2 ログ 2 (/en-us/federated-authentication-service/2511/media/fas-troubleshoot-logon-capi2-chainpolicy.png)

ドメインコントローラー セキュリティログ

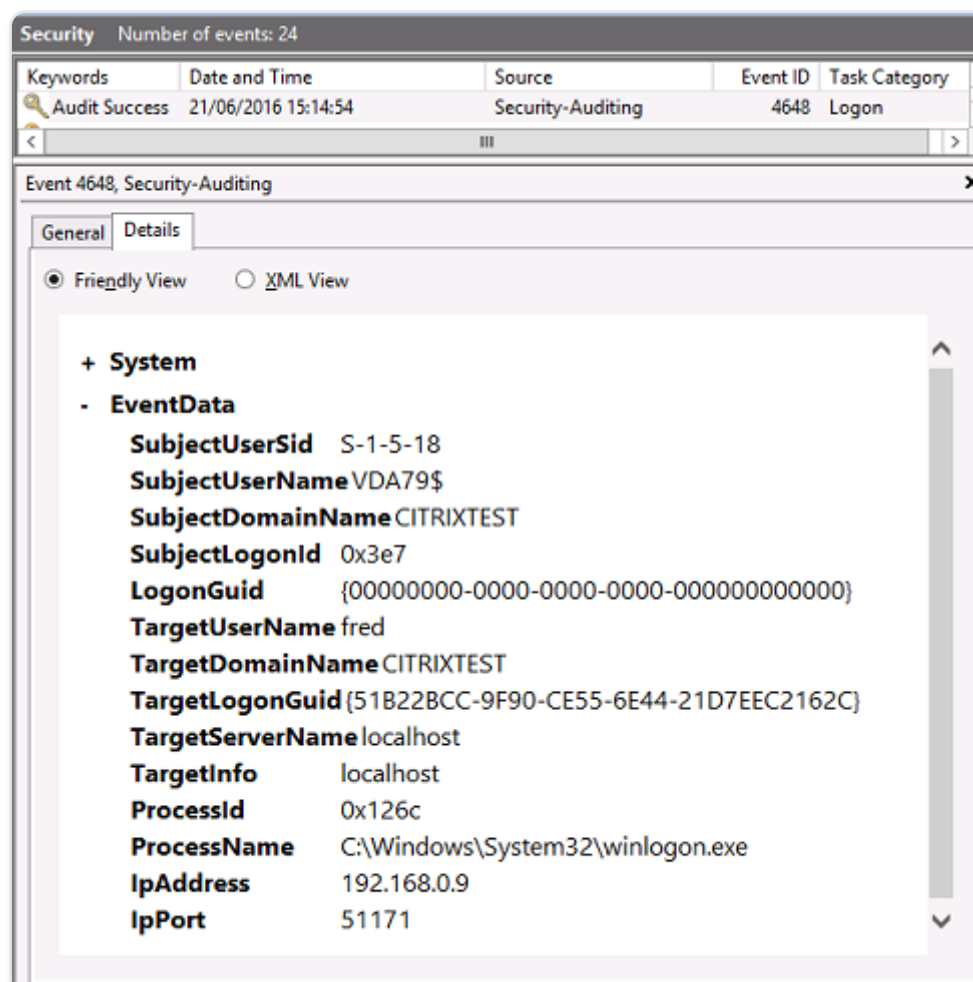
ドメインコントローラーは一連のログオンイベントを表示し、主要なイベントは4768です。このイベントでは、証明書がKerberosチケット保証チケット (krbtgt) の発行に使用されます。

これより前のメッセージは、サーバーのマシンアカウントがドメインコントローラーに対して認証を行っていることを示しています。これに続くメッセージは、新しい krbtgt に属するユーザーアカウントがドメインコントローラーに対して認証を行うために使用されていることを示しています。

ドメインコントローラー セキュリティログ (/en-us/federated-authentication-service/2511/media/fas-troubleshoot-logon-dc-security-log.png)

VDA セキュリティログ

ログオンイベントに対応するVDAセキュリティ監査ログは、winlogon.exeから発生するイベントID 4648のエントリです。



VDA CAPIログ

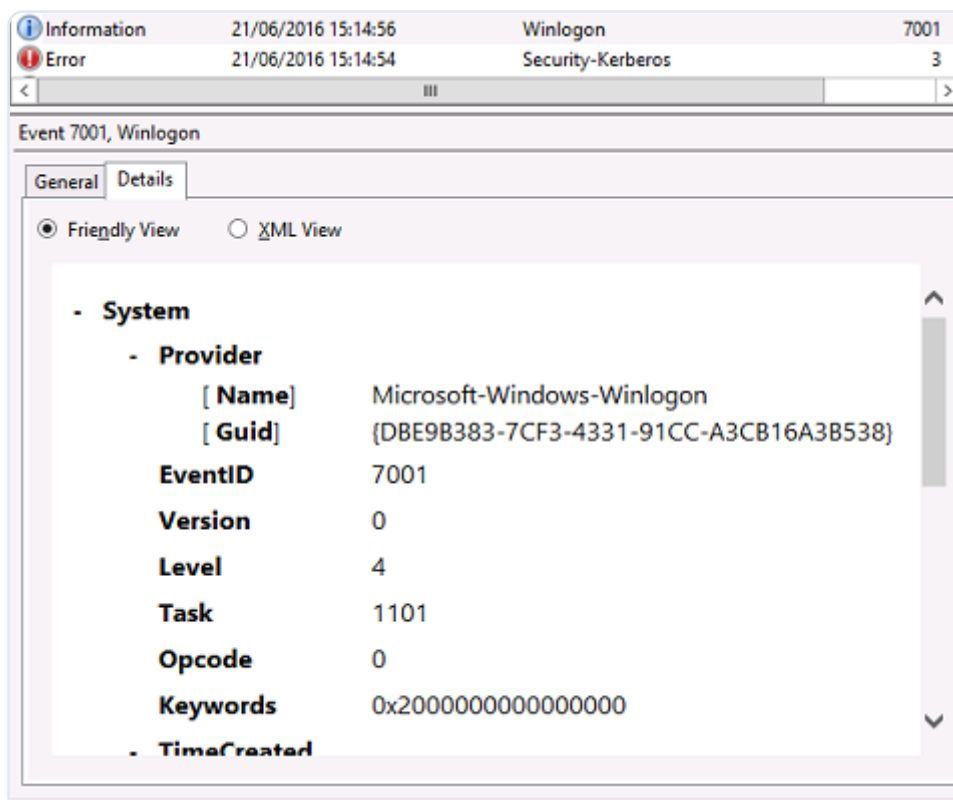
このVDA CAPIログの例は、lsass.exeからの単一のチェーン構築および検証シーケンスを示しており、ドメインコントローラー証明書 (dc.citrixtest.net) を検証しています。

Information	21/06/2016 15:14:54	CAPI2	30	Verify Chain P...
Information	21/06/2016 15:14:54	CAPI2	11	Build Chain
Information	21/06/2016 15:14:54	CAPI2	90	X509 Objects
Information	21/06/2016 15:14:54	CAPI2	41	Verify Revocat...
Information	21/06/2016 15:14:54	CAPI2	40	Verify Revocat...
Information	21/06/2016 15:14:54	CAPI2	10	Build Chain

- UserData	
- CertVerifyCertificateChainPolicy	
- Policy	
[type]	CERT_CHAIN_POLICY_NT_AUTH
[constant]	6
- Certificate	
[fileRef]	813C6D12E1E1800E61B8DB071E186EB912B7
[subjectName]	dc.citrixtest.net
- CertificateChain	
[chainRef]	{84E0B3D1-A4D4-4AC7-BA99-5291415B343}
- Flags	
[value]	0
- Status	
[chainIndex]	-1

VDAシステムログ

Kerberosログ記録が有効になっている場合、システムログにはエラー KDC_ERR_PREAUTH_REQUIRED (無視可能) と、Kerberosログオンが成功したことを示す Windowsログオンからのエントリが表示されます。



Windowsイベントログを使用したFASの監視

すべてのFASイベントは、Windowsのアプリケーションイベントログに書き込まれます。System Center Operations Manager (SCOM) などの製品を使用して、ここで説明されているプロセスとイベントを使用してFASサービスの正常性を監視できます。

FASサービスは実行中ですか？

FASサービスが実行中かどうかを判断するには、
Citrix.Authentication.FederatedAuthenticationService.exeプロセスを監視します。

FASサービスを監視するための最も重要なイベントのみがこのセクションで説明されています。
FASイベントコードの完全なリストについては、[FASイベントログ](#)を参照してください。

FASヘルスイベント

以下のイベントは、FASサービスが正常であるかどうかを示します。

イベントソースは **Citrix.Authentication.FederatedAuthenticationService** です。

イベント	イベントテキスト	説明	注
[S003]	管理者 [{0}] がメンテナンスモードを [{1}] に設定	FASサービスがメンテナンスモードに設定されたか、メンテナンスモードから解除されました。	メンテナンスモード中は、FASサーバーはシングルサインオンに使用できません。
[S022]	管理者 [{0}] がメンテナンスモードをオフに設定	FASサービスがメンテナンスモードから解除されました。	FAS 10.7 / Citrix Virtual Apps and Desktops 2109 以降で利用可能です。
[S023]	管理者 [{0}] がメンテナンスモードをオンに設定	FASサービスはメンテナンスモードになりました。	FAS 10.7 / Citrix Virtual Apps and Desktops 2109 から利用可能。
[S123]	[upn: {0} role: {1}] [exception: {2}] の証明書をいずれかのCAで発行できませんでした	このイベントは、FASが構成されているCAのいずれもユーザー証明書の発行に成功しなかった場合に、[S124] の後に発生します。そのユーザーのシングルサインオンは失敗します。	このイベントは、構成されているすべてのCAが機能していないことを示します。FASがHSMを使用するように構成されている場合、HSMが機能していないことも示している可能性があります。

イベント	イベントテキスト	説明	注
[S124]	[upn: {0} role: {1}] の証明書を [certificate authority: {2}] [exception: {3}] で発行できませんでした	FASが指定されたCAからユーザー証明書を要求しようとしたときに、エラーが発生しました。FASが複数のCAで構成されている場合、FASは別のCAで要求を試行します。	このイベントは、CAが機能していないか、連絡できないことを示している可能性があります。FASがHSMを使用するように構成されている場合、HSMが機能していないことも示している可能性があります。例外は、問題の原因を特定するのに役立ちます。
[S413]	承認証明書の有効期限が間もなく切れます（残り{0}日）。証明書の詳細: {1}	このイベントは、FAS承認証明書の有効期限が近づく定期的に生成されます。デフォルトでは、承認証明書の有効期限が30日以内である場合、イベントは毎日生成されます。	デフォルト設定は、cmdlet Set-FasRaCertificateMonitor を使用して調整できます。 「PowerShell cmdlet」 (/ja-jp/federated-authentication-service/2511/config-manage/ps-sdk.html) を参照してください。
[S414]	認証証明書の有効期限が切れました。証明書の詳細: {0}	FAS認証証明書の有効期限が切れると、このイベントが定期的に生成されます。デフォルトでは、このイベントは毎日生成されます。	有効期限が切れると、FASは新しいユーザー証明書を生成できなくなり、シングルサインオンが失敗し始めます。

クラウド接続FASイベント

Citrix Cloud™でFASを使用している場合、次のイベントはFASサービスが正常であるかどうかを示します。

イベントソースは **Citrix.Fas.Cloud** です。

イベント	イベントテキスト	説明	注
[S012]	Citrix CloudからのシングルサインオンにFASサービスが利用可能です	このイベントは、Workspace（つまりCitrix Cloud）からのシングルサインオンが機能しているはずであることを示します。	このイベントを発行する前に、FASは(1)構成されていること、(2)メンテナンスモードではないこと、および(3)Citrix Cloudに接続されていることを確認します。
[S013]	FASサービスはCitrix Cloudからのシングルサインオンに利用できません。[{0}] 詳細については、管理コンソールで確認できます。	このイベントは、FASがWorkspace（つまりCitrix Cloud）からのシングルサインオンを提供できないことを示しています。メッセージには、シングルサインオンが機能しない理由が含まれています。	FASはCitrix Cloudへの永続的な接続を維持します。この接続は、ネットワークの不具合やプロキシサーバーの接続寿命ポリシーなど、さまざまな理由で時々切断されることがあります。このような場合、イベントテキストには「Service is not connected to the cloud」と表示されます。これは通常の動作であり、FASはCitrix Cloudへの接続を直ちに再確立しようとします。

セキュリティイベント

次のイベントは、不正なエンティティがFASを使用しようとしたことを示しています。

イベントソースは **Citrix.Authentication.FederatedAuthenticationService** です。

イベント	イベントテキスト	説明
[S001]	アクセス拒否: ユーザー [{0}] はAdministratorsグループのメンバーではありません	FASの設定を表示または変更しようとしたが、呼び出し元はFAS管理者ではありませんでした。
[S002]	アクセス拒否: ユーザー [{0}] はロール [{1}] の管理者ではありません	FASルールの構成を表示または変更しようとしたが、呼び出し元はFAS管理者ではありませんでした。
[S101]	サーバー [{0}] は、役割 [{1}] でIDをアサートする権限がありません。	ユーザーIDをアサートしようとしたが、呼び出し元にはその権限がありません。 FASルールの構成で許可されているStoreFront™サーバー（および該当する場合はWorkspace）のみが、ユーザーIDをアサートできます。
[S104]	サーバー [{0}] はUPN [{1}] のアサートに失敗しました（UPNはルール [{2}] で許可されていません）。	ユーザーIDをアサートしようとしたが、FASルールの構成により、そのユーザーアカウントは許可されていません。
[S205]	依拠当事者アクセスが拒否されました - 呼び出し元アカウント [{0}] は、ルール [{1}] の許可された依拠当事者ではありません。	VDAがFASでシングルサインオンを実行しようとしたが、FASルールの構成により、そのVDAは許可されていません。

FASイベントログ

次の表に、FASによって生成されるイベントログエントリを示します。

管理イベント

これらのイベントは、FASサーバーでの構成変更に応じてログに記録されます。

ログコード
[S001] アクセス拒否: ユーザー [{0}] はAdministratorsグループのメンバーではありません
[S002] アクセス拒否: ユーザー [{0}] は役割 [{1}] の管理者ではありません
[S003] 管理者 [{0}] がメンテナンスモードを [{1}] に設定しています
[S004] 管理者 [{0}] がCA [{1}] からテンプレート [{2} and {3}] を使用して承認証明書を要求しています
[S005] 管理者 [{0}] がFAS承認 [RA cert id: {1}] を削除しています
[S006] 管理者 [{0}] が証明書定義 [{1}] を作成しています
[S007] 管理者 [{0}] が証明書定義 [{1}] を更新しています
[S008] 管理者 [{0}] が証明書定義 [{1}] を削除しています
[S009] 管理者 [{0}] がルール [{1}] を作成しています
[S010] 管理者 [{0}] がルール [{1}] を更新しています
[S011] 管理者 [{0}] がルール [{1}] を削除しています
[S012] 管理者 [{0}] が証明書 [upn: {1} sid: {2} rule: {3}] を作成しています [証明書定義: {4} セキュリティコンテキスト: {5}]
[S013] 管理者 [{0}] が証明書 [upn: {1} role: {2} Certificate Definition: {3} Security Context: {4}] を削除しています
[S015] 管理者 [{0}] が証明書要求 [TPM: {1}] を作成しています
[S016] 管理者 [{0}] が承認証明書をインポートしています [Reference: {1}]
[S022] 管理者 [{0}] がメンテナンスモードをオフに設定しています
[S023] 管理者 [{0}] がメンテナンスモードをオンに設定しています
[S024] 管理者 [{0}] がシステムヘルスマニターを設定しています
[S025] 管理者 [{0}] がシステムヘルスマニターを設定しています
[S026] 管理者 [{0}] がRA証明書モニターを設定しています

ログコード
[S027] 管理者 [{0}] がRA証明書モニターをリセットしています
[S028] 管理者 [{0}] が [{1}] 証明書のキー構成を [{2}] に設定しています
[S029] 管理者 [{0}] が [{1}] 証明書のキー構成をデフォルト値にリセットしています [{2}]
[S030] 管理者 [{0}] がサービスプロパティを [{1}] に設定しています
[S031] 管理者 [{0}] がCA [RA cert id: {1}] の承認を取り消しています
[S050] 管理者 [{0}] がクラウド構成を作成しています: [{1}]
[S051] 管理者 [{0}] がクラウド構成を更新しています: [{1}]
[S052] 管理者 [{0}] がクラウド構成を削除しています
[S060] 管理者 [{0}] がクラウド登録を要求しています。インスタンス: {1}
[S060] 管理者 [{0}] Direct Trust Cloud登録を要求しています。インスタンス: {1} CloudServiceUrlFormat: {2}
[S061] 管理者 [{0}] クラウド登録を完了しています。リソースの場所: {1}, ルール名: {2}
[S062] 管理者 [{0}] クラウド登録が完了しました。リソースの場所: {1} ({2}), ルール名: {3}, 顧客: {4} ({5})
[S063] クラウド登録中にKRSエラーが発生しました。例外は {0} でした。
[S064] クラウド登録中に不明なエラーが発生しました。例外は {0} でした。
[S065] 管理者 [{0}] Direct Trust Cloud登録を要求しています。インスタンス: {1} CloudServiceUrlFormat: {2}

ログコード
[S401] 構成のアップグレードを実行しています - [From version {0} to version {1}]
[S402] エラー: Citrix Federated Authentication ServiceはNetwork Serviceとして実行する必要があります [currently running as: {0}]
[S404] Citrix Federated Authentication Serviceデータベースを強制的に消去しています

ログコード
[S405] レジストリからデータベースへのデータ移行中にエラーが発生しました: [{0}]
[S406] レジストリからデータベースへのデータ移行が完了しました (注: ユーザー証明書は移行されません)
[S407] データベースが既に存在するため、レジストリベースのデータはデータベースに移行されませんでした
[S408] 構成をダウングレードできません -- [From version {0} to version {1}]
[S409] ThreadPoolの構成に成功しました - MinThreadsが [workers: {0} completion: {1}] から [workers: {2} completion: {3}] に調整されました
[S410] ThreadPool の構成に失敗しました - MinThreads を [workers: {0} completion: {1}] から [workers: {2} completion: {3}] に調整できませんでした。これは FAS サーバーのスケラビリティに影響を与える可能性があります。
[S411] FAS サービスの開始中にエラーが発生しました: [{0}]
[S412] 構成のアップグレードが完了しました -- [From version {0} to version {1}]
[S413] 認証証明書の有効期限が間もなく切れます (残り {0} 日)。証明書の詳細: {1}
[S414] 認証証明書の有効期限が切れました。証明書の詳細: {0}
[S415] 認証証明書の確認が完了しました。{0} 件の問題がログに記録されました。次回の確認は {1} に予定されています。

ID アサーションの作成

これらのイベントは、信頼されたサーバーがユーザーログオンをアサートするときに、FAS サーバーで実行時にログに記録されます。

ログコード
[S101] サーバー [{0}] は、ロール [{1}] で ID をアサートする権限がありません。
[S102] サーバー [{0}] は UPN [{1}] のアサートに失敗しました (例外: {2}{3})
[S103] サーバー [{0}] は UPN [{1}] SID {2} を要求しましたが、ルックアップは SID {3} を返しました。

ログコード
[S104] サーバー [{0}] は UPN [{1}] のアサートに失敗しました (UPN はルール [{2}] で許可されていません)
[S105] サーバー [{0}] は ID アサーションを発行しました [upn: {1}, role {2}, Security Context: [{3}]]
[S120] [upn: {0} role: {1} Security Context: [{2}]] に証明書を発行しています
[S121] [certificate authority: {2}] によって [upn: {0} role: {1}] に証明書が発行されました
[S122] 警告: サーバーが過負荷です [upn: {0} role: {1}][Requests per minute {2}]。
[S123] [upn: {0} role: {1}] [exception: {2}] のいずれの CA でも証明書の発行に失敗しました
[S124] [certificate authority: {2}] [exception: {3}] で [upn: {0} role: {1}] の証明書の発行に失敗しました
[S125] 保留中の証明書要求が完了するのを待機中に、{0} 秒後に呼び出しがタイムアウトしました [upn: {1} role: {2} Security Context: [{3}]]
[S126] サーバー [{0}] は、未定義のルール [{1}] を使用してIDをアサートしようとしてしました
[S127] サーバーがメンテナンスモードであるため、FASは [upn: {0} role: {1} definition: {2}] の証明書を要求できませんでした。メンテナンスモード中の動作を変更するには、PowerShell コマンド レット Set-FasServer を使用してください

証明書利用者として機能する

これらのイベントは、VDA がユーザーをログオンするときに、FAS サーバーで実行時にログに記録されます。

ログコード
[S201] 証明書利用者 [{0}] にはパスワードへのアクセス権がありません。
[S202] 証明書利用者 [{0}] には証明書へのアクセス権がありません。
[S203] 証明書利用者 [{0}] にはログオンプロバイダーへのアクセス権がありません
[S204] 依頼当事者 [{0}] が [upn: {1}] のログオンプロバイダーに [{2}] の役割でアクセスしています。 [Operation: {3}] 承認元: [{4}]

ログコード
[S205] 依頼当事者のアクセスが拒否されました - 呼び出し元のアカウント [{0}] は、ルール [{1}] の許可された依頼当事者ではありません
[S206] 呼び出し元のアカウント [{0}] は依頼当事者ではありません
[S208] 秘密鍵操作が失敗しました [Operation: {0} upn: {1} role: {2} certificateDefinition {3} Error {4} {5}].
[S209] キャッシュされた証明書が見つかりません。[Caller: {0}] [upn: {1}] [role: {2}] [cert definition: {3}] [Operation: {4}]

セッション内証明書サーバー

ユーザーがセッション内証明書を使用すると、これらのイベントがFASサーバーに記録されます。

ログコード
[S301] アクセス拒否: ユーザー [{0}] は仮想スマートカードへのアクセス権がありません
[S302] ユーザー [{0}] が不明な仮想スマートカード [thumbprint: {1}] を要求しました
[S303] アクセス拒否: ユーザー [{0}] は仮想スマートカード [upn: {1}] と一致しません
[S304] ユーザー [{0}] がコンピューター [{2}] でプログラム [{1}] を実行し、秘密鍵操作 [{6}] に仮想スマートカード [upn: {3} role: {4} thumbprint: {5}] を使用しています
[S305] 秘密鍵操作が失敗しました [Operation: {0}] [upn: {1} role: {2} containerName {3} Error {4} {5}]。

FASアサーションプラグイン

これらのイベントは、FASアサーションプラグインによってログに記録されます。

ログコード
[S500] FASアサーションプラグインが構成されていません
[S501] 構成されたFASアサーションプラグインをロードできませんでした [exception:{0}]
[S502] FASアサーションプラグインがロードされました [pluginId={0}] [assembly={1}] [location={2}]

ログコード
[S503] サーバー [{0}] はUPN [{1}] のアサートに失敗しました (ログオン証拠が提供されましたが、プラグイン [{2}] はそれをサポートしていません)
[S504] サーバー [{0}] はUPN [{1}] のアサートに失敗しました (ログオン証拠が提供されましたが、構成されたFASプラグインがありません)
[S505] サーバー [{0}] はUPN [{1}] のアサートに失敗しました (プラグイン [{2}] はログオン証拠をステータス [{3}] とメッセージ [{4}] で拒否しました)
[S506] プラグイン [{0}] は、サーバー [{1}] からのUPN [{2}] のログオン証拠をメッセージ [{3}] で受け入れました
[S507] サーバー [{0}] はUPN [{1}] のアサートに失敗しました (プラグイン [{2}] はメソッド [{4}] の実行中に例外 [{3}] をスローしました)
[S507] サーバー [{0}] はUPN [{1}] のアサートに失敗しました (プラグイン [{2}] は例外 [{3}] をスローしました)
[S508] サーバー [{0}] はUPN [{1}] のアサートに失敗しました (アクセス処理が提供されましたが、プラグイン [{2}] はそれをサポートしていません)
[S509] サーバー [{0}] はUPN [{1}] のアサートに失敗しました (アクセス処理が提供されましたが、構成されたFASプラグインがありません)
[S510] サーバー [{0}] はUPN [{1}] のアサートに失敗しました (アクセス処理はプラグイン [{2}] によって無効と見なされました)

ワークスペース対応FAS

これらのイベントは、FASがWorkspaceで使用されているときにログに記録されます。

ログコード
[S001] Citrix Cloud認証キーがローテーションされました [fas id: {0}] [old key id:{1}] [new key id: {2}]
[S002] クラウドサポートモジュールが起動しています。FasHubクラウドサービスURL: {0}
[S003] FASがクラウドに登録されました [fas id: {0}] [transaction id: {1}]
[S004] FASのクラウドへの登録に失敗しました [fas id: {0}] [transaction id: {1}] [exception: {2}]

ログコード
[S005] FASが現在の構成をクラウドに送信しました [fas id: {0}] [transaction id: {1}]
[S006] FASの現在の構成のクラウドへの送信に失敗しました [fas id: {0}] [transaction id: {1}] [exception: {2}]
[S007] FASがクラウドから登録解除されました [fas id: {0}] [transaction id: {1}]
[S009] FASのクラウドからの登録解除に失敗しました [fas id: {0}] [transaction id: {1}] [exception: {2}]
[S010] FASサービスはクラウドメッセージングURLに接続されています: {0}
[S011] FASサービスはクラウドに接続されていません
[S012] FASサービスはCitrix Cloudからのシングルサインオンに利用可能です
[S013] FASサービスはCitrix Cloudからのシングルサインオンに利用できません。[{0}] 詳細については、管理コンソールで確認できます。
[S014] クラウドサービスへの呼び出し <service name> は失敗しました [fas id: {0}] [transaction id: {1}] [exception: {2}]
[S015] 呼び出し元が許可されていないため、Citrix Cloudからのメッセージがブロックされました [message ID {0}] [transaction ID {1}] [caller {2}]
[S016] クラウドサービスへの呼び出し <service name> は成功しました [fas id: {0}] [transaction id: {1}]
[S019] FASはクラウドから構成をダウンロードしました [fas id: {0}] [transaction id: {1}]
[S020] FASはクラウドから構成をダウンロードできませんでした [fas id: {0}] [transaction id: {1}] [exception: {2}]
[S021] クラウドサポートモジュールの起動に失敗しました。例外: {0}
[S022] クラウドサポートモジュールを停止しています
[S023] Citrix Cloud認証キーのローテーションに失敗しました [fas id: {0}] [current key id:{1}] [new key id:{2}] [keys in cloud:{3}]
[S024] Citrix Cloud認証キーのローテーションを開始しています [fas id: {0}] [current key id:{1}] [new key id:{2}]

ログコード
[S025] このサービスの認証キーはCitrix Cloudに存在します [current key: {0}] [keys in cloud: {1}]
[S026] このサービスの認証キーはCitrix Cloudに存在しません [current key: {0}] [keys in cloud: {1}]
[S027] Citrix Cloud認証キーのストレージ形式をアップグレードしました [fas id: {0}]
[S028] FASは現在のテレメトリをクラウドに送信しました [fas id: {0}] [transaction id: {1}]
[S029] FASは現在のテレメトリをクラウドに送信できませんでした [fas id: {0}] [transaction id: {1}] [exception: {2}]

ログオン

これらのイベントは、ログオン段階中にVDAに記録されます。

ログコード
[S101] IDアサーションログオンに失敗しました。認識されないフェデレーション認証サービス GPOインデックス [index: {0}] [registry name: {1}]
[S102] IDアサーションログオンに失敗しました。{0}のSIDルックアップに失敗しました [Exception: {1}{2}]
[S103] IDアサーションログオンに失敗しました。ユーザー{0}のSIDは{1}ですが、予期されるSIDは{2}です
[S104] IDアサーションログオンに失敗しました。{0}への呼び出しは [Error: {1} {2}] を返しました
[S105] IDアサーションログオン。ログオン中 [Username: {0} Domain: {1}]
[S106] IDアサーションログオン。\\n\\nフェデレーション認証サービス: {0}\\n\\nログオン中 [Certificate: {1}]
[S107] IDアサーションログオンに失敗しました。 [Exception: {0}{1}]
[S108] IDアサーションサブシステム。アクセス拒否 [Caller: {0}]

セッション内証明書

これらのイベントは、ユーザーがセッション内証明書を使用しようとしたときにVDAに記録されます。

ログコード
[{0}] が [PID: {1} Program Name: {2}Certificate thumbprint: {3}] のために [S201] 仮想スマートカードアクセスを承認しました
[S203] 仮想スマートカードサブシステム。アクセス拒否 [caller: {0}, session {1}]
[S204] 仮想スマートカードサブシステム。スマートカードサポートが無効になっています

証明書要求とキーペアの生成

これらのイベントは、FASサーバーが低レベルの暗号化操作を実行するときにログに記録されます。

ログコード
[S001] TrustArea::TrustArea: 証明書をインストールしました [TrustArea: {0} Certificate {1} TrustAreaJoinParameters {2}]
[S014] Pkcs10Request::Create: PKCS10要求を作成しました [Distinguished Name: {0}] [Reason: {1}]
[S016] 秘密鍵の作成 [Identifier: {0}] [MachineWide: {1}] [Provider: {2}] [ProviderType: {3}] [EllipticCurve: {4}] [KeyLength: {5}] [isExportable: {6}] [CreateReason: {7}]
[S017] プライベートキーの削除 [Provider: {0}] [Identifier {1}] [Twin: {2}]
[S018] PrivateKey::Create が失敗しました [Identifier: {0}] [MachineWide: {1}] [Provider: {2}] [ProviderType: {3}] [EllipticCurve: {4}] [KeyLength: {5}] [isExportable: {6}] [CreateReason: {7}] [Exception: {8}]

ログコード
[S104] FASはCA {0} から承認証明書を受信しました。
[S105] MicrosoftCertificateAuthority::SubmitCertificateRequest 応答の送信エラー [{0}]
[S106] MicrosoftCertificateAuthority::SubmitCertificateRequest 証明書を発行しました [{0}]
[S112] MicrosoftCertificateAuthority::SubmitCertificateRequest - 承認待ち [CR_DISP_UNDER_SUBMISSION] [Reference: {0}]

エンドユーザーのエラーメッセージ

このセクションでは、Windowsログオンページでユーザーに表示される一般的なエラーメッセージを一覧表示します。

表示されたエラーメッセージ	説明と参照
無効なユーザー名またはパスワード	コンピューターは有効な証明書と秘密鍵を持っていると認識していますが、Kerberosドメインコントローラーが接続を拒否しました。この記事の *Kerberosログ* セクションを参照してください。
システムがログオンできませんでした。資格情報を検証できませんでした。 / 要求はサポートされていません	ドメインコントローラーに接続できないか、ドメインコントローラーがスマートカード認証をサポートする証明書で構成されていません。ドメインコントローラーを「Kerberos認証」、「ドメインコントローラー認証」、または「ドメインコントローラー」証明書に登録してください。既存の証明書が有効に見える場合でも、これは試す価値があります。
システムがログオンできませんでした。認証に使用されたスマートカード証明書は信頼されていませんでした。	中間証明書とルート証明書がローカルコンピューターにインストールされていません。 証明書と公開鍵インフラストラクチャ を参照してください。
不正な要求	これは通常、証明書の拡張機能が正しく設定されていないか、RSAキーが短すぎる (<2048 ビット) ことを示します。

FAS 常時トレース

常時トレースを使用すると、FAS はそのアクティビティをファイルシステムにログ記録します。これはトラブルシューティングに役立ち、発生したインシデントを再現する必要性を排除できる可能性があります。

常時トレースは、以下のいずれかの方法を使用して FAS をインストールまたはアップグレードすると有効になります。

- Citrix Virtual Apps and Desktops™ インストーラー: ISO が挿入されたときの自動実行スプラッシュ画面の **Federated Authentication Service** ボタンから

- `XenDesktopFasSetup.exe` : Citrix Virtual Apps and Desktops ISO の `x64\XenDesktop Setup\XenDesktopFasSetup.exe` にあります
- `FasSetup_xxxx.exe` : スタンドアロンの FAS インストーラーファイル。Citrix Downloads から入手できます。

注：

FAS インストーラー MSI ファイル `FederatedAuthenticationService_x64.msi` を使用してインストールまたはアップグレードする場合、常時トレースは利用できません。

常時トレースの収集

FAS サーバーから常時トレースおよびその他の診断データを収集するには、[Citrix Scout](#) を使用します。**Citrix Scout** は、前述のいずれかの方法を使用して FAS をインストールするとインストールされます。

常時トレースの無効化

何らかの理由で常時トレースを無効にしたい場合は、FAS サーバーで **Citrix Telemetry Service** を停止して無効にします。

常時トレースを中央ログサーバーに送信する

詳細および構成手順については、[AOT の記事](#) を参照してください。

関連情報

- [スマートカードログオン用にドメインを構成する](#)
- [スマートカードログオンポリシー](#)
- [CAPIログ記録を有効にする](#)
- [Kerberosログ記録を有効にする](#)
- サードパーティの認証局でスマートカードログオンを有効にするためのガイドライン(<https://support.microsoft.com/ja-jp/kb/281245>)

PowerShell コマンドレット

シンプルな展開には Federated Authentication Service (FAS) 管理コンソールを使用できますが、PowerShell インターフェースはより高度なオプションを提供します。コンソールで利用できない

オプションを使用する予定がある場合は、Citrix は構成に PowerShell のみを使用することを推奨します。

次のコマンドは、FAS PowerShell コマンドレットを追加します。

```
Add-PSSnapin Citrix.Authentication.FederatedAuthenticationService.V1
```

PowerShell ウィンドウで、`Get-Help \<cmdlet name>` を使用してコマンドレットのヘルプを表示できます。

FAS PowerShell SDK コマンドレットの詳細については、[<https://developer-docs.citrix.com/projects/federated-authentication-service-powershell-cmdlets/en/latest/>](https://developer-docs.citrix.com/projects/federated-authentication-service-powershell-cmdlets/en/latest/) を参照してください。

FASインストーラーオプション

FASをインストールするためのコマンドラインオプション

次のオプションは、両方で有効です。

1. Citrix Virtual Apps and Desktops ISOの `x64\XenDesktop Setup\XenDesktopFasSetup.exe` にある `XenDesktopFasSetup.exe` ファイル
2. `FasSetup_xxxx.exe` (xxxxは[Citrix Downloads](#)から入手可能なリリース)

- `/configure_firewall`

Windowsファイアウォールサービスが実行されている場合、ファイアウォールが有効になっていなくても、インストールされているコンポーネントで使用するWindowsファイアウォールのすべてのポートを開きます。サードパーティのファイアウォールを使用している場合、またはファイアウォールを使用していない場合は、手動でポートを開く必要があります。FASには、受信TCPポート80が必要です。

- `/help or /h or /? ?`

コマンドヘルプを表示します。

- `/noreboot`

インストール後の再起動を防止します。

- `/quiet` または `/passive`

インストール中にユーザーインターフェイスは表示されません。インストールおよび構成プロセスの唯一の証拠は、Windowsタスクマネージャーにあります。このオプションを省略すると、グラフィカルインターフェイスが起動します。

- `/remove`

FASを削除します。

- `/installdir`

インストールフォルダーを指定します。

コンポーネントインストールの結果をCitrixがどのように報告するかについては、「[Citrix インストールリターンコード](#)」を参照してください。

Windows Server CoreへのFASのインストール

Citrix Virtual Apps and Desktops ISO、またはスタンドアロンのFASインストーラーexe (`FasSetup_xxxx.exe`) が、FASをインストールするための推奨される方法です。ただし、有効になっているOS機能によっては、Windows Server Coreにこれらを使用してインストールできない場合があります。

代わりに、Citrix Virtual Apps and Desktops™ ISOから以下のMSIファイルを使用してください。

MSIファイル	ISO上の場所	コメント
<code>FederatedAuthenticationService_x64.msi</code>	<code>x64\Federated Authentication Service</code>	必須
<code>TelemetryServiceInstaller_x64.msi</code>	<code>x64\Virtual Desktop Components</code>	推奨。常時トレースのサポートを提供します。

前提条件として、`.net4.8` がインストールされている必要があります。

インストールまたはアップグレードするには、次のコマンドを使用します。

```
msiexec /i FederatedAuthenticationService_x64.msi [/quiet]
CONFIGUREFIREWALL=[YES|NO]

msiexec /i TelemetryServiceInstaller_x64.msi [/quiet]

net start "Citrix Telemetry Service"
```

オプションは次のとおりです。

- `/quiet` : ユーザーインターフェイスを表示しません
- `CONFIGUREFIREWALL`: ファイアウォールを構成して、ポート80での受信接続を許可する場合は**YES**を指定します。このオプションを省略した場合のデフォルトは**NO**です。

FASを削除するには、次のコマンドを使用します。

```
msiexec /x FederatedAuthenticationService_x64.msi [/quiet]

msiexec /x TelemetryServiceInstaller_x64.msi [/quiet]
```

Windows Server CoreでのFAS管理

FASは、ローカルまたはFASがインストールされている別のコンピューターから、次のいずれかの方法で構成および管理できます。

- [FAS PowerShell コマンドレット](#)
- [FAS管理コンソールGUI](#)

PowerShellコマンドレットを使用する場合は、`-Address` パラメーターをターゲットFASサーバーのFQDNに設定します。または、変数 `$CitrixFasAddress` をFQDNに設定することもできます。ローカルFASを管理する場合は、**localhost**を指定できます。

FAS管理コンソールを使用する場合は、右上隅にある**Connect to another server**リンクをクリックします。

展開アーキテクチャ

はじめに

Federated Authentication Service (FAS) is a Citrix® component that integrates with your Active Directory certificate authority, allowing users to be seamlessly authenticated within a Citrix environment. This document describes various authentication architectures that may be appropriate for your deployment.

When enabled, FAS delegates user authentication decisions to trusted StoreFront servers. StoreFront has a comprehensive set of built-in authentication options built around modern web technologies, and is easily extensible using the StoreFront SDK or third-party IIS plugins. The basic design goal is that any authentication technology that can authenticate a user to a web site can now be used to log in to a Citrix Virtual Apps or Citrix Virtual Desktops™ deployment.

このドキュメントでは、複雑さが増すにつれて、トップレベルの展開アーキテクチャの例について説明します。

- [内部展開](#)
- [シトリックス ゲートウェイ展開](#)
- [ADFS SAML](#)
- [B2B アカウントマッピング](#)
- [ウィンドウズ 10 Azure AD 参加](#)

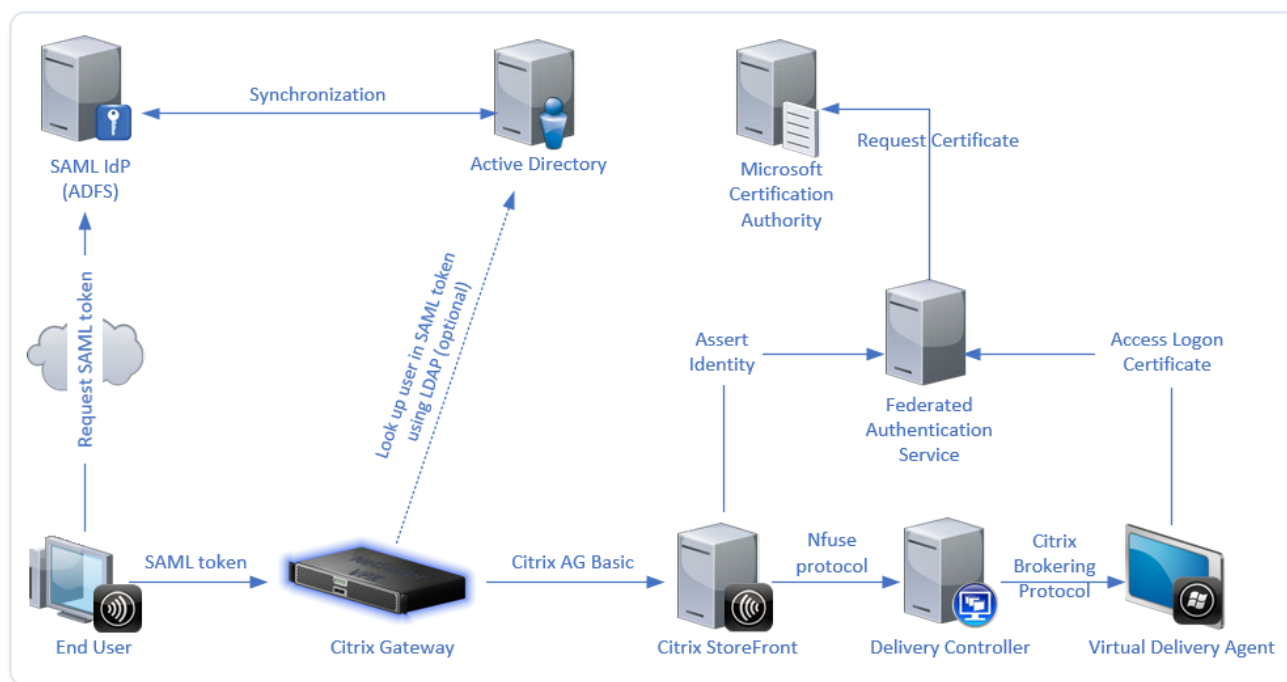
関連するFAS記事へのリンクが提供されています。すべてのアーキテクチャにおいて、FASのセットアップに関する主要なリファレンスは[インストールと構成](#)の記事です。

アーキテクチャの概要

FASは、StoreFrontによって認証されたActive Directoryユーザーに代わって、スマートカードクラスの証明書を自動的に発行することを承認されています。これは、管理者が物理スマートカードをプロビジョニングできるツールと同様のAPIを使用します。ユーザーがCitrix Virtual Apps™またはCitrix Virtual Desktops Virtual Delivery Agent (VDA)に仲介されると、証明書がマシンに添付され、Windowsドメインはログオンを標準のスマートカード認証として認識します。

信頼されたStoreFront™サーバーは、ユーザーがCitrix環境へのアクセスを要求すると、FASに接続します。FASは、そのセッションの証明書を使用して、単一のCitrix Virtual AppsまたはCitrix Virtual Desktopsセッションを認証できるチケットを付与します。VDAがユーザーを認証する必要がある場合、FASに接続してチケットを引き換えます。FASのみがユーザー証明書の秘密キーにアクセスできます。VDAは、証明書で実行する必要がある署名および復号化操作をすべてFASに送信する必要があります。

次の図は、FASがMicrosoft Certification Authorityと統合し、StoreFrontおよびCitrix Virtual Apps and Desktops™ Virtual Delivery Agents (VDAs)にサポートサービスを提供している様子を示しています。



内部展開

FAS を使用すると、ユーザーはさまざまな認証オプション（Kerberos シングルサインオンを含む）を使用して StoreFront に安全に認証し、完全に認証された Citrix HDX™ セッションに接続できます。

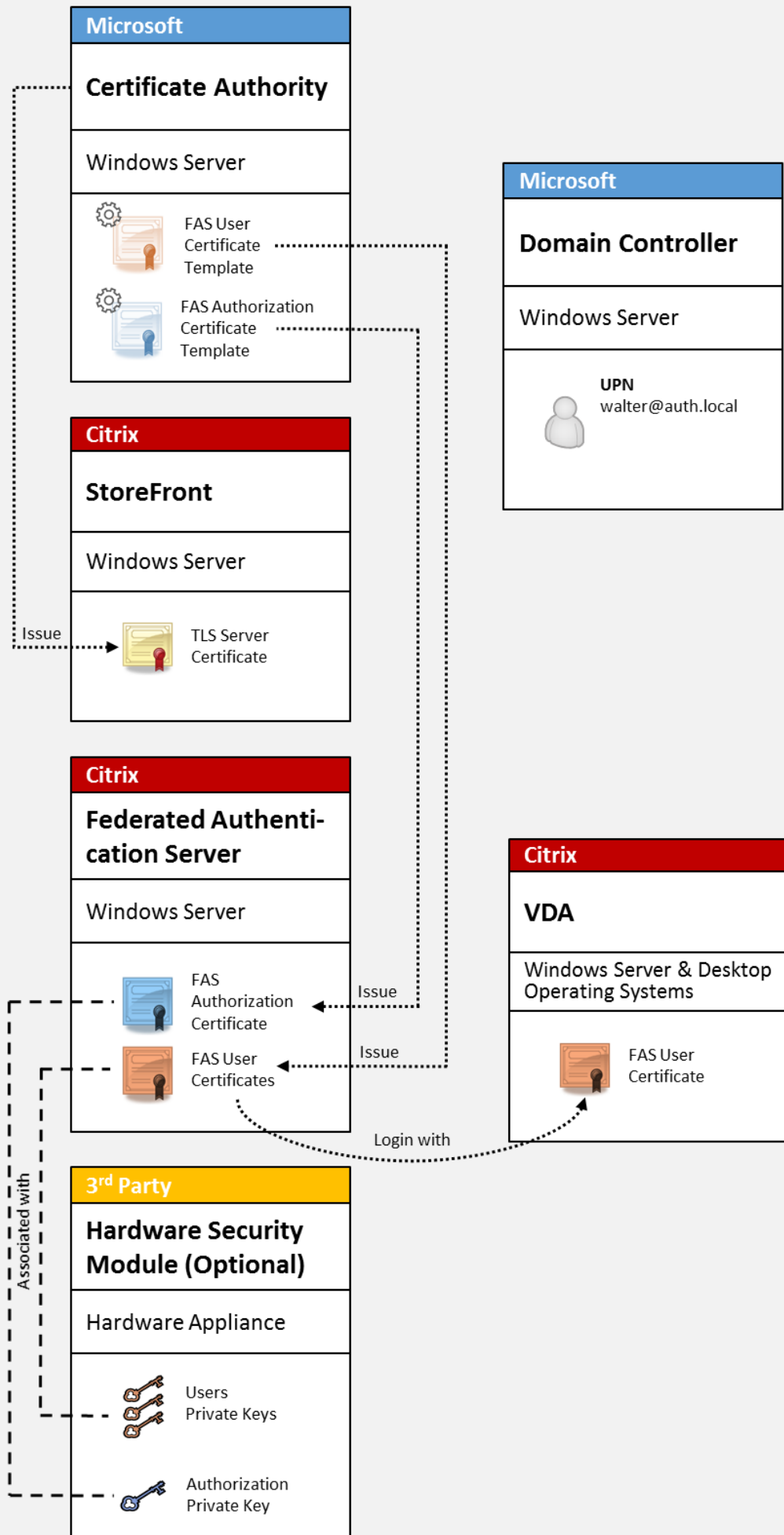
これにより、ユーザー資格情報やスマートカードの PIN を入力するプロンプトなしで、またシングルサインオンサービスなどの「保存されたパスワード管理」機能を使用せずに Windows 認証が可能になります。これは、以前のバージョンの Citrix Virtual Apps で利用可能だった Kerberos 制限付き委任ログオン機能を置き換えるために使用できます。

すべてのユーザーは、エンドポイントデバイスにスマートカードでログオンしているかどうかにかかわらず、セッション内で公開鍵インフラストラクチャ（PKI）証明書にアクセスできます。これ

により、スマートカードリーダーを持たないスマートフォンやタブレットなどのデバイスからでも、二要素認証モデルへのスムーズな移行が可能になります。

この展開では、FAS を実行する新しいサーバーが追加され、このサーバーはユーザーに代わってスマートカードクラスの証明書を発行する権限を持ちます。これらの証明書は、スマートカードログオンが使用されたかのように、Citrix HDX 環境のユーザーセッションにログオンするために使用されます。

AUTH.LOCAL domain



Citrix Virtual Apps または Citrix Virtual Desktops 環境は、スマートカードログオンと同様の方法で構成する必要があります。これについては、[CTX206156](#) に記載されています。

既存の展開では、通常、ドメインに参加している Microsoft 証明機関が利用可能であり、ドメインコントローラーにドメインコントローラー証明書が割り当てられていることを確認するだけです。（[CTX206156](#) の「ドメインコントローラー証明書の発行」セクションを参照してください。）

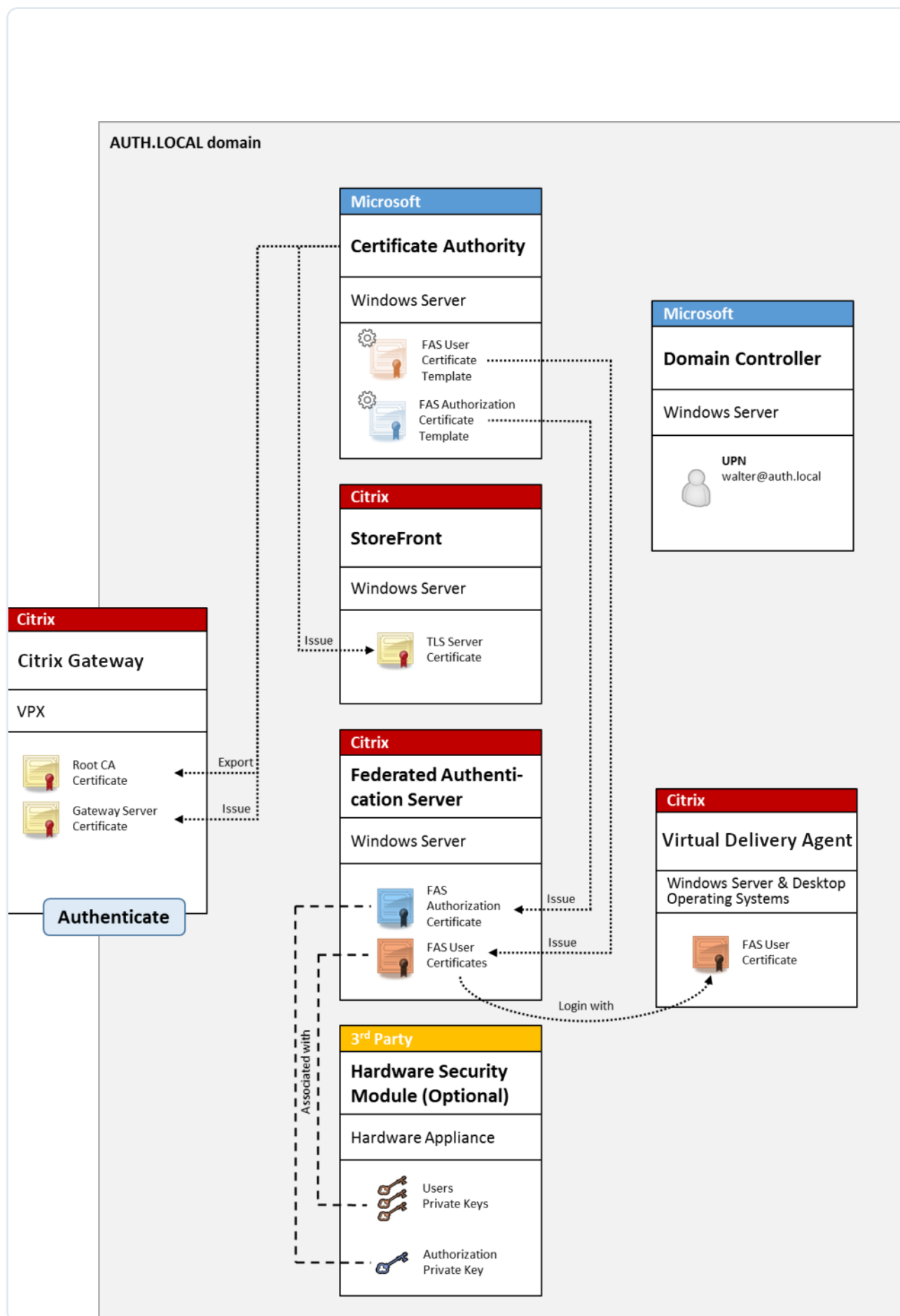
関連情報:

- キーは、ハードウェアセキュリティモジュール（HSM）または組み込みのトラステッドプラットフォームモジュール（TPM）に保存できます。詳細については、[秘密キーの保護](#) の記事を参照してください。
- [インストールと構成](#) の記事では、FAS のインストール方法と構成方法について説明しています。

Citrix Gateway の展開

Citrix Gateway の展開は内部展開と似ていますが、StoreFront とペアリングされた Citrix Gateway が追加され、認証の主要なポイントが Citrix Gateway 自体に移されます。Citrix Gateway には、企業の Web サイトへのリモートアクセスを保護するために使用できる高度な認証および承認オプションが含まれています。

この展開は、最初に Citrix Gateway に認証し、その後ユーザーセッションにログオンする際に発生する複数の PIN プロンプトを回避するために使用できます。また、AD パスワードやスマートカードを別途必要とせずに、高度な Citrix Gateway 認証テクノロジーを使用することもできます。



Citrix Virtual AppsまたはCitrix Virtual Desktops環境は、スマートカードログオンと同様の方法で構成する必要があります。これはCTX206156に記載されています。

既存の展開では、通常、ドメイン参加済みのMicrosoft証明機関が利用可能であり、ドメインコントローラーにドメインコントローラー証明書が割り当てられていることを確認するだけで済みます。（CTX206156の「ドメインコントローラー証明書の発行」セクションを参照してください）。

Citrix Gatewayをプライマリ認証システムとして構成する場合、Citrix GatewayとStoreFront間のすべての接続がTLSで保護されていることを確認してください。特に、コールバックURLがCitrix Gatewayサーバーを指すように正しく構成されていることを確認してください。これは、この展開でCitrix Gatewayサーバーを認証するために使用できます。

Add NetScaler Gateway Appliance

StoreFront

- ✓ General Settings
- ✓ Secure Ticket Authority
- Authentication Settings**
- Summary

Authentication Settings

These settings specify how the remote user provides authentication credentials

Version: 10.0 (Build 69.4) or later

VServer IP address: (optional) v10.0: SNIP or MIP, v10.1+: VIP

Logon type: i Domain

Smart card fallback: None

Callback URL: i (optional) https://NetScalerGatewayFQDN /CitrixAuthService/AuthService.asmx

⚠ When no Callback URL is specified, Smart Access is not available.

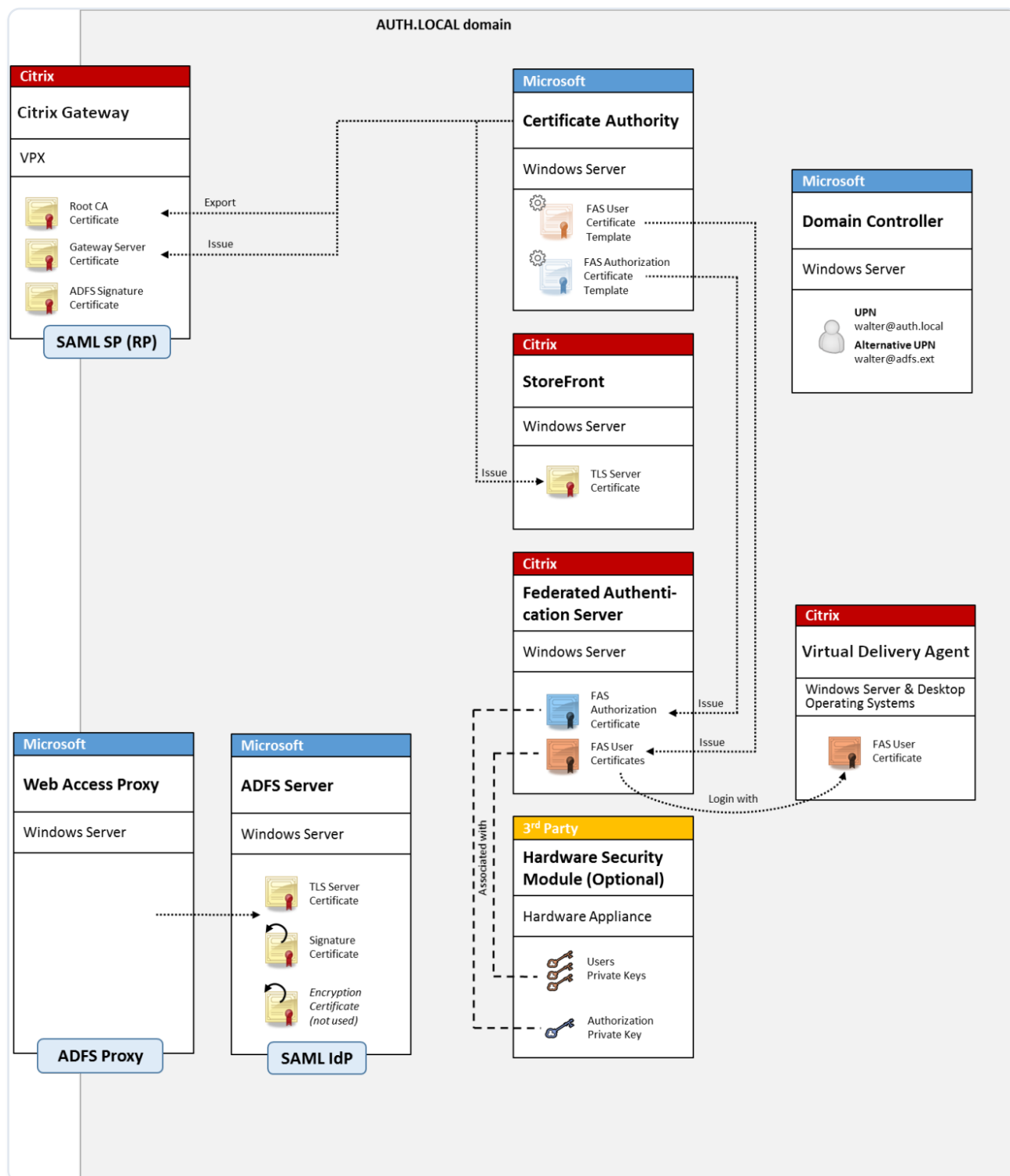
Back Create Cancel

関連情報:

- Citrix Gatewayを構成するには、"[How to Configure NetScaler Gateway 10.5 to use with StoreFront 3.6 and Citrix Virtual Desktops 7.6](#)"を参照してください。
- [Install and configure](#)は、FASのインストールと構成方法について説明しています。

ADFS SAML展開

主要なCitrix Gateway認証テクノロジーは、SAML IDプロバイダー (IdP) として機能できるMicrosoft ADFSとの統合を可能にします。SAMLアサーションは、信頼されたIdPによって発行される暗号署名されたXMLブロックであり、ユーザーがコンピューターシステムにログオンすることを承認します。これは、FASサーバーがユーザーの認証をMicrosoft ADFSサーバー（またはその他のSAML対応IdP）に委任できることを意味します。



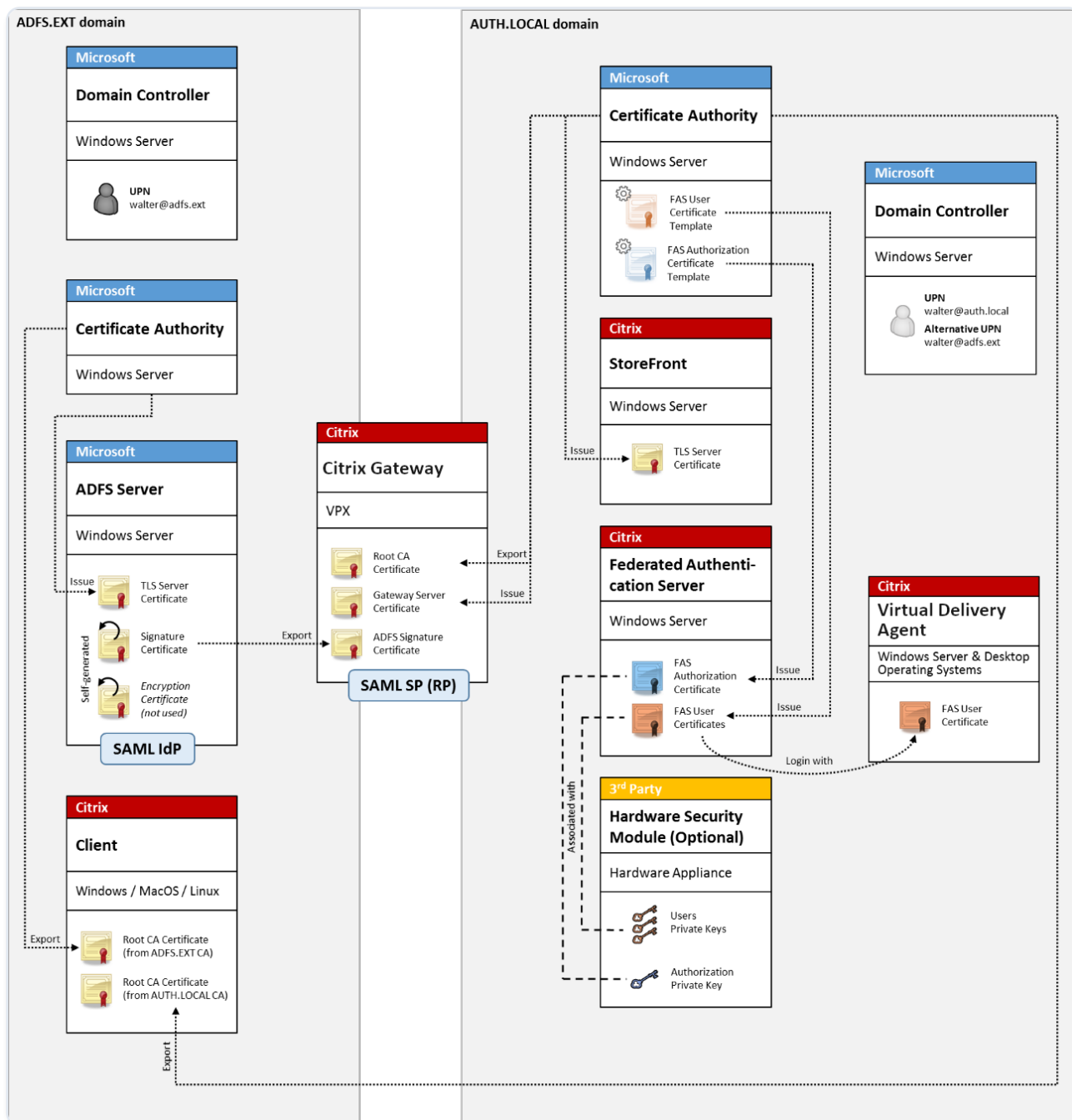
ADFSは、インターネット経由でリモートから企業リソースにユーザーを安全に認証するためによく使用されます。たとえば、Office 365統合によく使用されます。

関連情報:

- [ADFS deployment](#)の記事に詳細が記載されています。
- [Install and configure](#)の記事は、FASのインストールと構成方法について説明しています。
- この記事の[Citrix Gateway展開](#)セクションには、構成に関する考慮事項が含まれています。

B2Bアカウントマッピング

2つの会社が互いのコンピューターシステムを使用したい場合、一般的な選択肢は、信頼関係を持つActive Directory Federation Service (ADFS) サーバーをセットアップすることです。これにより、ある会社のユーザーが別の会社のActive Directory (AD) 環境にシームレスに認証できるようになります。ログオン時、各ユーザーは自身の会社のログオン資格情報を使用し、ADFSはこれをピア会社のAD環境内の「シャドウアカウント」に自動的にマッピングします。



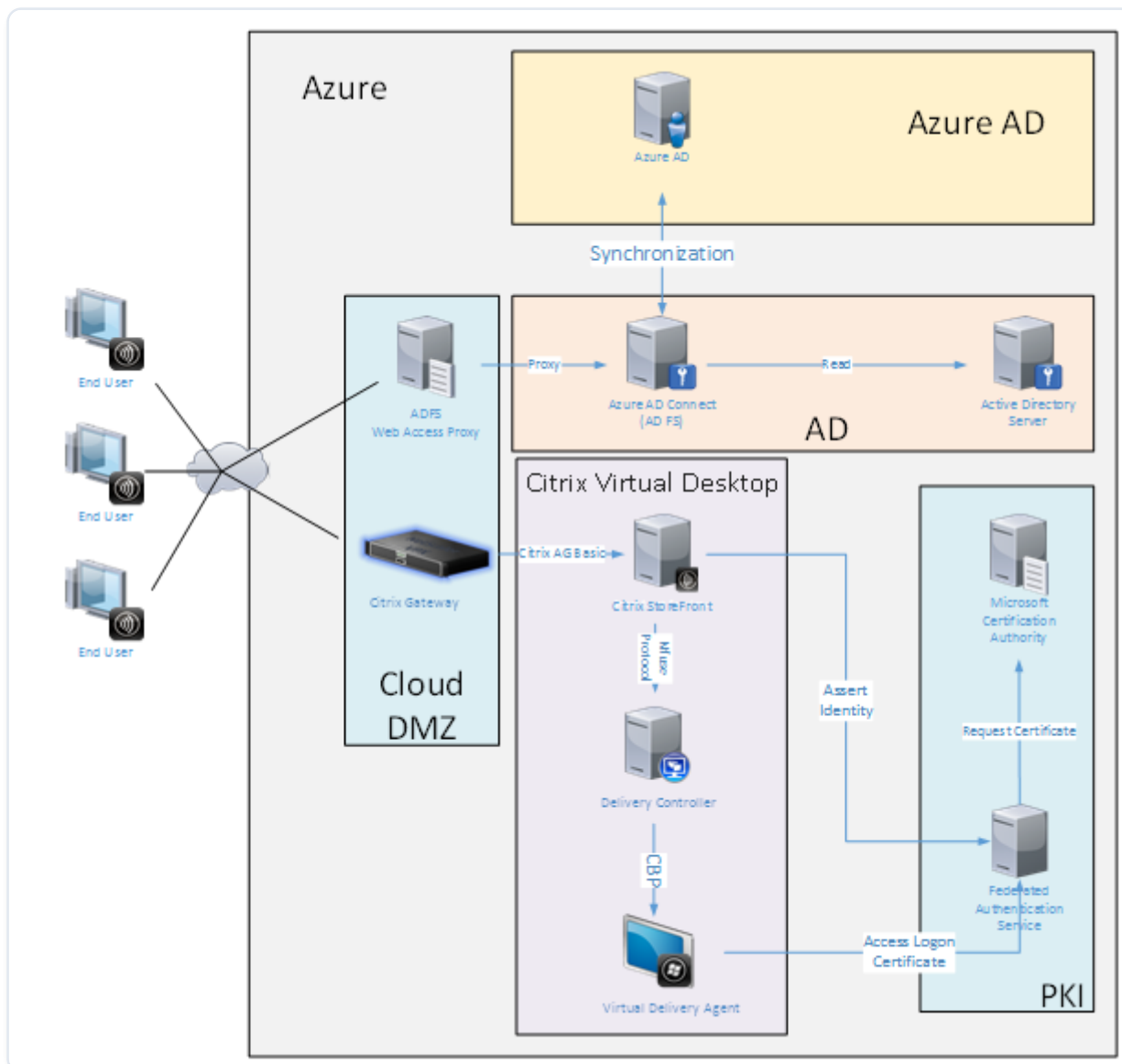
関連情報:

- [インストールと構成](#)の記事では、FASのインストールと構成方法について説明しています。

Windows 10 Azure AD への参加

Windows 10では、「Azure AD Join」という概念が導入されました。これは、従来のWindowsドメイン参加と概念的には似ていますが、「インターネット経由」のシナリオを対象としています。これはラップトップやタブレットでうまく機能します。従来のWindowsドメイン参加と同様に、Azure ADには会社のウェブサイトやリソースに対するシングルサインオンモデルを可能にする

る機能があります。これらはすべて「インターネット対応」であるため、オフィスLANだけでなく、インターネットに接続されたあらゆる場所から機能します。



この展開は、「オフィス内のエンドユーザー」という概念が実質的に存在しない例です。ラップトップは、最新のAzure AD機能を使用して、完全にインターネット経由で登録および認証されます。

この展開のインフラストラクチャは、IPアドレスが利用可能な場所であればどこでも実行できることに注意してください。オンプレミス、ホスト型プロバイダー、Azure、またはその他のクラウドプロバイダーです。Azure AD Connectシンクロナイザーは自動的にAzure ADに接続します。簡素化のため、例のグラフィックではAzure VMを使用しています。

関連情報:

- [インストールと構成](#)の記事では、FASのインストールと構成方法について説明しています。

ADFS展開

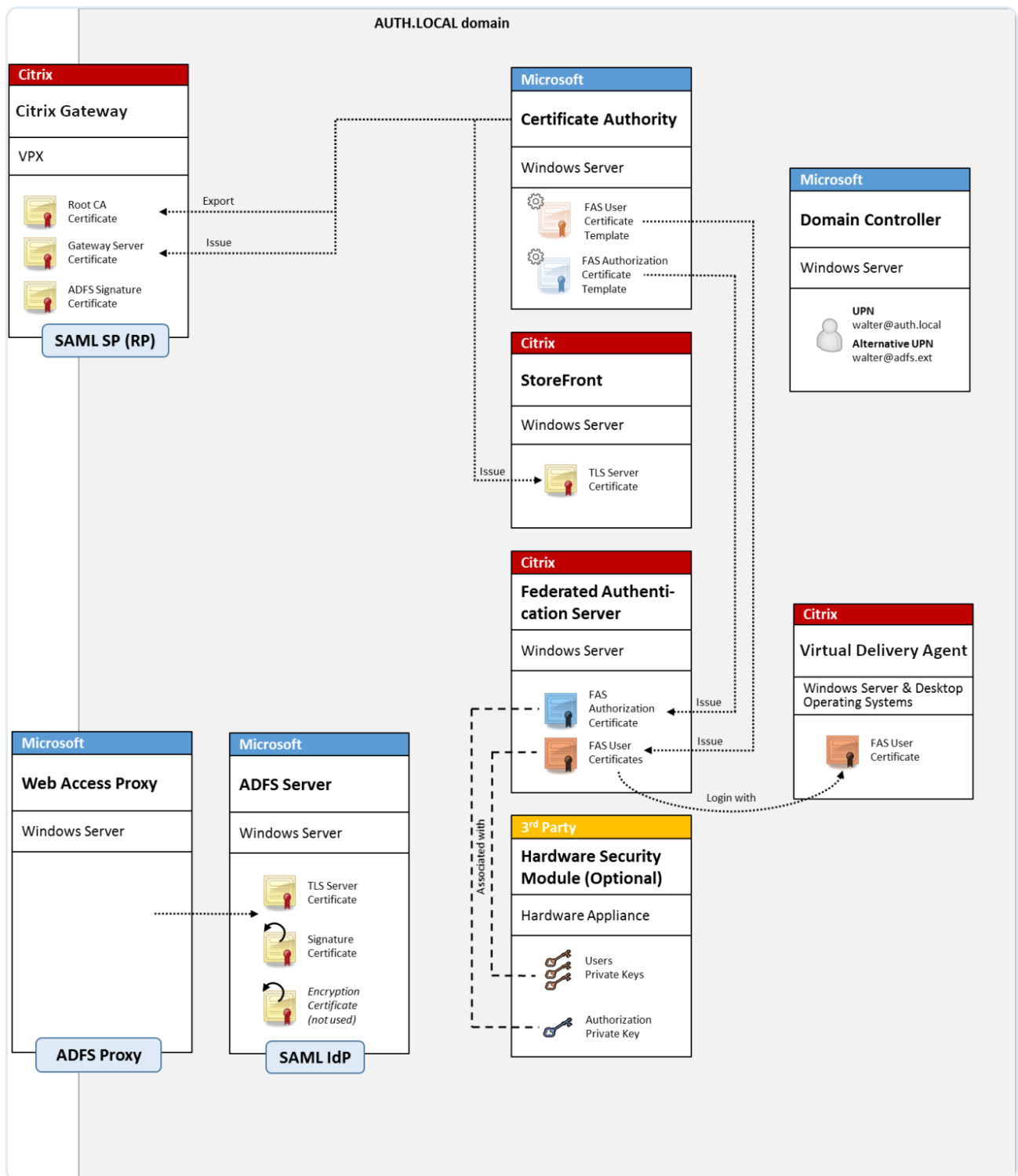
はじめに

このドキュメントでは、Citrix環境をMicrosoft ADFSと統合する方法について説明します。

多くの組織では、単一の認証ポイントを必要とするWebサイトへの安全なユーザーアクセスを管理するためにADFSを使用しています。たとえば、企業は従業員が利用できる追加のコンテンツやダウンロードを持っている場合があります。これらの場所は、標準のWindowsログオン資格情報で保護する必要があります。

Federated Authentication Service (FAS) は、Citrix Gateway と Citrix StoreFront™ を ADFS ログオンシステムと統合することも可能にし、従業員の潜在的な混乱を軽減します。

この展開では、Citrix Gateway を Microsoft ADFS の証明書利用者として統合します。



注：

バックエンドリソースがWindows VDAまたはLinux VDAのどちらであっても、違いはありません。

SAMLの概要

Security Assertion Markup Language (SAML) は、シンプルな「ログオンページへのリダイレクト」Webブラウザログオンシステムです。構成には次の項目が含まれます。

リダイレクトURL

Citrix Gateway は、ユーザーが認証される必要があることを検出すると、ユーザーのWebブラウザに、ADFSサーバー上のSAMLログオンWebページにHTTP POSTを実行するように指示します。これは通常、`https://` の形式のアドレスです: `https://adfs.mycompany.com/adfs/ls`。

このWebページPOSTには、ログオン完了時にADFSがユーザーを返す「戻りアドレス」を含むその他の情報が含まれています。

識別子

EntityIdは、Citrix GatewayがADFSへのPOSTデータに含める一意の識別子です。これは、ユーザーがどのサービスにログオンしようとしているかをADFSに通知し、必要に応じて異なる認証ポリシーを適用します。発行された場合、SAML認証XMLはEntityIdによって識別されるサービスへのログオンにのみ適しています。

通常、EntityIdはCitrix GatewayサーバーのログオンページのURLですが、Citrix GatewayとADFSが合意していれば、一般的には何でも構いません。 `https://ns.mycompany.com/application/logonpage`。

戻りアドレス

認証が成功すると、ADFSはユーザーのWebブラウザに、EntityId用に構成された応答URLのいずれかにSAML認証XMLをPOSTするよう指示します。これは通常、元のCitrix Gatewayサーバー上の `https://` アドレスで、形式は次のとおりです。 `https://ns.mycompany.com/cgi/samlauth`。

複数の応答URLアドレスが構成されている場合、Citrix GatewayはADFSへの最初のPOSTでいずれかを選択できます。

署名証明書

ADFSは、秘密鍵を使用してSAML認証XMLプロブに暗号署名します。この署名を検証するには、Citrix Gatewayが証明書ファイルに含まれる公開鍵を使用してこれらの署名をチェックするように構成されている必要があります。証明書ファイルは通常、ADFSサーバーから取得したテキストファイルです。

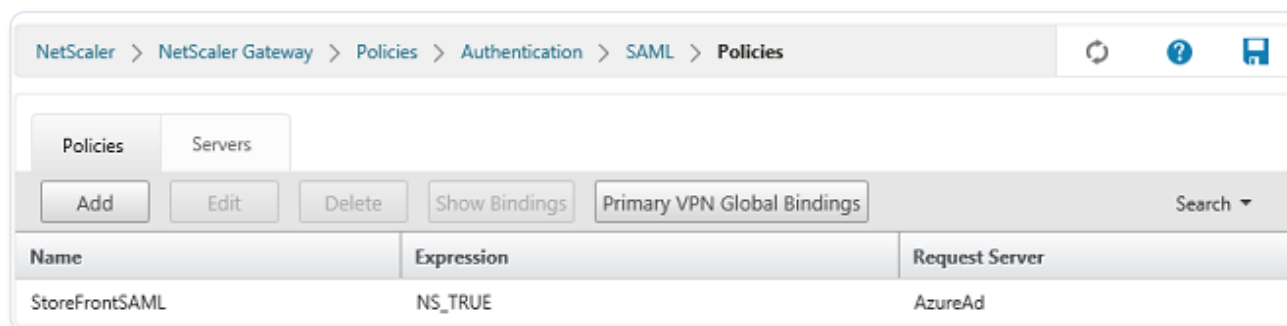
シングルサインアウトURL

ADFSとCitrix Gatewayは「中央ログアウト」システムをサポートしています。これは、Citrix GatewayがSAML認証XMLプロブが現在ログオンしているセッションをまだ表しているかどうかを確認するために時々ポーリングするURLです。

これは、構成する必要のないオプション機能です。通常、`https://` アドレスで、形式は `https://adfs.mycompany.com/adfs/logout` です。(シングルログオンURLと同じにすることもできます。)

構成

セクション [Citrix Gatewayの展開](#) では、標準のLDAP認証オプションを処理するようにCitrix Gatewayを設定する方法について説明しています。それが正常に完了した後、SAML認証を許可する新しい認証ポリシーをCitrix Gateway上に作成できます。これは、Citrix Gatewayウィザードで使用されるデフォルトのLDAPポリシーを置き換えることができます。



SAMLポリシーを記入する

以前にADFS管理コンソールから取得した情報を使用して、新しいSAML IdPサーバーを構成します。このポリシーが適用されると、Citrix GatewayはユーザーをADFSにリダイレクトしてログオンさせ、ADFS署名付きSAML認証トークンを受け入れます。

Create Authentication SAML Server

Create Authentication SAML Server

Name*
AzureAd

Authentication Type
SAML

IDP Certificate Name*
AzureADSAML

Redirect URL*
29f-4c20-9826-14d5e484c62e/saml2

Single Logout URL
29f-4c20-9826-14d5e484c62e/saml2

User Field
userprincipalname

Signing Certificate Name

Issuer Name
https://ns.citrixsaml demo.net/Citrix/

Reject Unsigned Assertion*
ON

SAML Binding*
POST

Default Authentication Group

Skew Time(mins)
5

5

Two Factor
☐ ON ☒ OFF

Assertion Consumer Service Index
255

Attribute Consuming Service Index
255

Requested Authentication Context*
Exact

Authentication Class Types
InternetProtocol
InternetProtocolPassword

Signature Algorithm*
☐ RSA-SHA1 ☒ RSA-SHA256

Digest Method*
☐ SHA1 ☒ SHA256

☐ Send Thumbprint
☒ Enforce Username

Attribute 1
Attribute 3
Attribute 5
Attribute 7

Attribute 1
Attribute 3
Attribute 5
Attribute 7

関連情報

- [インストールと構成](#) は、FAS のインストールと構成に関する主要なリファレンスです。
- 一般的な FAS 展開は、[展開アーキテクチャ](#) の記事にまとめられています。
- 「ハウツー」記事は、[高度な構成](#) の記事で紹介されています。